REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
27-10-2010	FINAL	

4. TITLE AND SUBTITLE
A Case for Principles of Cyberspace Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

David W. Snoddy, Lt Col, USAF

Paper Advisor: Mark E. Donahue, CAPT, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT
The requirement to conduct deliberate military operations in the cyberspace domain is a relatively recent addition to the U.S. armed forces' mission set yet joint doctrine for the planning and execution of operations within cyberspace has not been published. This paper concludes specific principles for cyberspace operations should be developed to serve as the foundation from which the doctrine can be developed. The case supporting this conclusion is grounded on a number of key points. First, the current principles of war are not as timeless and universal as they are often perceived to be. Second, there is a precedent within U.S. joint doctrine for establishing operation and domain-specific principles. Finally, an examination of the cyberspace attack on Georgia in 2008 illustrates how a principle called precision would be more useful for planning and executing cyberspace operations than the traditional principle mass. The paper concludes by recommending U.S. Cyber Command lead the development of a tailored set of principles of cyberspace operations which will serve to guide the planning and execution of joint operations in cyberspace with the ultimate objective of enabling U.S. forces to retain freedom of action while denying the same to our adversaries.

15. SUBJECT TERMS
Principles of War, Cyberspace, Cyberspace Operations

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		26	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

A Case for Principles of Cyberspace Operations

by

David W. Snoddy

Lieutenant Colonel, USAF

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

27 October 2010

Contents

Abstract

The requirement to conduct deliberate military operations in the cyberspace domain is a relatively recent addition to the U.S. armed forces‟ mission set yet joint doctrine for the planning and execution of operations within cyberspace has not been published. This paper concludes specific principles for cyberspace operations should be developed to serve as the foundation from which the doctrine can be developed. The case supporting this conclusion is grounded on a number of key points. First, the current principles of war are not as timeless and universal as they are often perceived to be. Second, there is a precedent within U.S. joint doctrine for establishing operation and domain-specific principles. Finally, an examination of the cyberspace attack on Georgia in 2008 illustrates how a principle called *precision* would be more useful for planning and executing cyberspace operations than the traditional principle *mass*. The paper concludes by recommending U.S. Cyber Command lead the development of a tailored set of principles of cyberspace operations which will serve to guide the planning and execution of joint operations in cyberspace with the ultimate objective of enabling U.S. forces to retain freedom of action while denying the same to our adversaries.

INTRODUCTION

The requirement to conduct deliberate military operations in the cyberspace domain is a relatively recent addition to the U.S. armed forces‟ mission set. Specifically, policy documents such as the 2004 *National Military Strategy* established the concept that U.S. armed forces must be able to operate in the cyberspace domain just as they operate across the domains of land, sea, air, and space.[1] On 23 June 2009 the Secretary of Defense directed the establishment of U.S. Cyber Command (USCYBERCOM) as a sub-unified command under U.S. Strategic Command and it achieved initial operational capability 21 May 2010 under the command of General Keith Alexander.[2] Despite the emphasis the creation of a dedicated cyberspace command implies, joint doctrine for the planning and execution of operations within cyberspace has not been published.[3] Given these facts, there is a clear and pressing need to develop comprehensive joint doctrine for cyberspace operations.

Logically, all doctrine should be grounded on core principles. Considering we are on the ground floor with respect to conceptualizing doctrine for cyberspace operations, one has to ask the question: are the current core principles underlying joint doctrine, the principles of war, applicable and sufficient for operations in cyberspace? This paper will argue the answer to the question is no, the principles of war are not sufficient for operations within the cyberspace domain and principles for cyberspace operations should be developed.

Before developing the case in support of the aforementioned assertion, the counter argument that the current principles of war are in fact a sufficient foundation for cyberspace operations will be presented. Following that, the concept of cyberspace as a domain will be explored and a working definition of cyberspace operations will be presented to focus the analysis which will follow. Next, a brief history of the origins of the principles of war will be presented.

With those key concepts as a backdrop, the case for the development of *principles of cyberspace operations* will be made as follows. First, the analysis will show the current principles of war are not as timeless and universal as they are often perceived to be. Second, it will show there is a precedent within joint doctrine for establishing operation and domain-specific principles. Finally, as one example to support the assertion, the analysis will conclude by illustrating how a principle called *precision* would be more useful for planning and executing cyberspace operations than the traditional principle *mass*.

COUNTER ARGUMENTS

The time-tested principles of war will ultimately apply in cyberspace.

— General Keith Alexander, USA, "Warfighting in Cyberspace"

The principles of war are often considered to be universal, timeless principles which are applicable regardless of the domain in which operations are conducted. This view has been generally espoused with respect to cyberspace by General Alexander and by former Secretary of the Air Force Michael Wynne.[4] Beyond these general statements, a number of military scholars have made this same argument.

Major David Farmer, USAF, examined how the principles of war apply in cyberspace by first exploring the history of the principles of war and describing cyber war. He then examined each principle in turn to determine whether the existing principles of war "adequately address the nature of cyber war."[5] His conclusion was: "the Principles of War do apply to cyber war and there is no need to develop additional principles."[6]

Lieutenant Colonel Sebastian Convertino, USAF, et al. explored many aspects of cyberspace operations but the one of interest here is their conclusion that: "the principles of war are supported through the application of cyber capabilities, both directly and as enablers. Cyberspace capabilities do not change the nature of war."[7] To support their conclusion, they

presented a table which enumerates the principles of war and lists a *sample cyber capability application* applicable to each principle without additional discussion or explanation.[8] The fundamental reason for this approach appears to be the implied notion that the principles of war are sacrosanct and represent the very nature of war.

While detailed joint doctrine has yet to be published for cyberspace operations, the United States Air Force published a dedicated doctrine document, *Cyberspace Operations,* Air Force Doctrine Document (AFDD) 3-12 in July 2010. The new document contains a table which lists the principles of joint operations (of which the principles of war are a subset) and lists an *example cyberspace operation* for each principle.[9] For example, the *example cyberspace operation* provided for maneuver is: "Use of numerous IPs to avoid attribution during a cyber attack."[10] As with the study by Convertino et al., there is no further discussion exploring the linkage between cyberspace operations and the principles of war which suggests AFDD 3-12"s authors accepted the principles of war to be applicable.

CYBERSPACE AND CYBERSPACE OPERATIONS DEFINED

> *Freedom of action in cyberspace...is crucial to the efficient employment of one's forces in all domains.*
>
> — General Keith Alexander, USA, "Warfighting in Cyberspace"

The Cyberspace Domain

The term *cyberspace* has existed in society for a number of years. However, the concept of cyberspace as a domain in which military operations can be conducted is relatively new. As with the adoption of any new concept, associated definitions have been developed and introduced within the military lexicon. Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms,* officially defines *cyberspace* as: "A global domain within the information environment consisting of the interdependent network of

information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[11]

Cyberspace has a number of attributes which mark it as a distinctly different operational environment than the other traditional military domains. A basic understanding of these attributes will aid in understanding the discussion and analysis which follows.

Cyberspace Is Manmade. The first attribute worth noting is cyberspace is a manmade phenomenon; consequently, it requires human action to persist.[12]

Cyberspace Does Not Equal the Electromagnetic Spectrum. The electromagnetic spectrum is a key natural phenomenon upon which portions of cyberspace‟s infrastructure depends for its existence; however, the electromagnetic spectrum does not equal cyberspace.

Cyberspace Nodes Exist in All Other Domains. The physical equipment which makes up cyberspace exists in and supports operations in all of the other natural domains.

Operational Costs Are Low in Cyberspace. The costs associated with the procurement of cyberspace capabilities are very low compared to the costs of procuring military hardware to operate in the other traditional military domains. Additionally, software code, tools, and techniques useful to an adversary in cyberspace are freely available on the Internet.

Cyberspace Does Not Have Meaningful Geographic Boundaries. The very nature of the infrastructures which constitute cyberspace (particularly the Internet) means cyberspace operations will, in many instances, be conducted against or through network infrastructure owned by commercial or foreign government entities and located at points all around the globe; more often than not, not even in the geographic area where an adversary is located.[13]

Attribution Is Very Difficult in Cyberspace. The very diverse and largely commercial nature of the structure of cyberspace, combined with restrictions in international law and

government policy, make it difficult if not impossible to attribute hostile actions conducted in cyberspace to a specific hostile actor, whether it is a hacker or a state-sponsored actor.[14]

Cyberspace Superiority Is Not a Certainty. The cumulative effect of the preceding attributes makes achieving superiority in cyberspace a challenge. The 2006 *National Military Strategy for Cyberspace Operations* stated: "Although the United States currently enjoys technological advantages in cyberspace, these advantages are eroding. Unlike the other warfighting domains, the United States risks parity with adversaries."[15] Some are even more pessimistic. Dr. Lani Kass, the director of a Cyber Task Force established by the Air Force in 2006, stated "the United States is perhaps fifth in the world in the cyber domain."[16]

Cyberspace Operations

With a fundamental description of cyberspace and several relevant attributes now established, it is appropriate to focus on defining what it means to conduct military operations in cyberspace. Some discussions on cyberspace operations broadly over generalize its scope. Suggesting all military use of cyberspace constitutes militarily relevant cyberspace operations is like saying all use of land is militarily relevant. For example, land is used to grow crops and it serves as a foundation for the buildings we live and work in yet the acts of farming and construction do not become land operations simply because they take place on and make use of land. It is more useful to view cyberspace operations as distinct, planned actions taken to achieve an objective rather than simply as any action conducted in or reliant on cyberspace. Accordingly, JP 1-02 defines cyberspace operations as: "the employment of cyber capabilities where the primary purpose is to achieve objectives in or through cyberspace. Such operations include computer network operations and activities to operate and defend the Global Information Grid."[17]

Those familiar with the doctrinal construct for information operations (IO) will note there is a term embedded within the preceding definition which is familiar; specifically, computer network operations (CNO) which is also a core IO capability.[18] This overlap could lead to the erroneous conclusion that cyberspace operations are in fact just a new name for CNO within the overarching construct of IO. While both IO and cyberspace operations may employ CNO to achieve their objectives, it is the objectives themselves which distinguish whether IO or cyberspace operations are being conducted. The focus of IO is on affecting "adversarial human and automated decision making while protecting our own."[19] In contrast, the principal focus of cyberspace operations is to use cyberspace to attack the adversary"s information technology infrastructure with the intent to deny freedom of action in cyberspace while protecting our own freedom of action.[20] Simply put, information operations seek to affect decision making while cyberspace operations seek to affect freedom of action in cyberspace.

THE UTILITY AND ORIGINS OF THE PRINCIPLES OF WAR

> *It [principles] gives us a sort of short-hand, wherein a mere phrase can convey a very considerable body of thought and mutual understanding.*
>
> — Bernard Brodie, "The Worth of Principles of War"

Now that a concept for what constitutes cyberspace operations has been established, the principles of war need to be similarly examined to provide a foundation for the case for distinct principles of cyberspace operations.

The Utility of Principles of War

A scan through joint doctrine reveals wide use of the term *principle*. In other words, there are many more principles elaborated within joint doctrine than the nine defined principles of war (which are a subset of the principles of joint operations.) As a matter of

fact, we could derive from the following excerpt from JP 1, *Doctrine for the Armed Forces of the United States,* that codifying principles is a fundamental purpose of joint doctrine: "Joint doctrine presents fundamental principles that guide the employment of US military forces in coordinated and integrated action toward a common objective."[21]

Given the fact there are many principles described in joint doctrine, it is important to understand the relevance of the nine defined principles of war beyond the simple fact they are principles. The fact they are separated and distinct from all of the other identified principles suggests there is something different about them worth noting. JP 1 explains their purpose as follows: "Conducting joint operations generally involves 12 broad principles, collectively known as the „principles of joint operations." These principles guide warfighting at the strategic, operational, and tactical levels of war. They combine the nine historical principles of war (present in joint doctrine since its inception) with three additional principles born out of experience across the range of military operations."[22]

With the above-listed JP 1 quotes as background, we can surmise the principles of war are not intended to provide cookbook or checklist solutions for operational planners when designing campaigns; rather, they are to serve as a commonly understood set of historically-derived truisms among planners which should guide their planning. The preceding quote refers to the principles of war as "historical" and having been "present in joint doctrine since its inception." This begs the question, where exactly did the principles of war come from?

The Origins of the Principles of War

Throughout history, military scholars have studied the conduct of war and most of them referenced principles or some variant thereof in their writings. John Alger, in his book *The Quest for Victory,* presents the single most comprehensive history of the concept of principles of war, starting with the writings of Sun Tzu in 500 BC and working forward

through history, presenting 68 distinct examples of documented principles of the military art. Alger notes an interesting distinction which is, prior to the time of Napoleon, none of the theorists developed or presented a specific list or attempted to specify exactly how many principles there were.[23] Alger describes the shift in conception of the principles of war which occurred during Napoleon's era as follows: "Rather than representing a commonly accepted philosophy concerning the myriad activities that collectively compose the operations of war, the term [principles of war] began to connote a brief list of aphorisms intended to guide commanders."[24]

The adoption and inclusion of a formalized list of principles of war in U.S. military doctrine was driven by the U.S. Army and Alger provides the following summary:

> The term "principles of war" has been repeatedly used and abandoned in U.S. Army handbooks and manuals. It first appeared in U.S. doctrine in the U.S. Army *Training Regulations* of the 1920s, but criticism of the form and to a lesser extent of the content of the *Training Regulations* list led to doctrine in the early 1930s that intentionally avoided the use of the term "principles of war." In 1931 however, the "principles of offensive combat," a list of ten aphorisms, appeared in an army manual, *Tactics and Techniques of Infantry in Offensive Combat.* In many cases the principles in this list were identical with "principles of war" that had appeared in *Training Regulations.* In 1936, the U.S. Army Command and General Staff College at Fort Leavenworth, Kansas, published a list of seven "principles of strategy," in substance identical to seven of the nine "principles of war" found in *Training Regulations*. In 1939, the staff college published a pamphlet, *The Offensive*, in which six "principles of war" appeared. Again the six repeated in form and content ideas that had been included in earlier U.S. Army doctrinal sources under different headings. In 1941, a similar list of seven aphorisms appeared under a unique heading, "The exercise of Command; Doctrines of Combat," and in 1949, the U.S. Army *Field Service Regulations*, at the time the most general doctrinal source in the U.S. Army, published a list of nine titles and explanations—again under the heading "principles of war."[25]

The nine titled principles in the 1949 list exactly match the titles of the principles of war listed in joint doctrine today. However, while the titles have remained consistent, the descriptions of various principles have been changed over time.

With the key concepts of cyberspace and cyberspace operations defined and the utility and origins of the principles of war now established, the case for the development of principles of cyberspace operations will now be made.

THE CASE FOR PRINCIPLES OF CYBERSPACE OPERATIONS

> *Now is the time to update our doctrine to establish fundamental cyber warfare principles.*
>
> — General Keith Alexander, "Warfighting in Cyberspace"

The principles of war were derived and codified largely based on historical combat experience in land warfare. Simply extending those principles to the domain of cyberspace without critical analysis of their applicability or sufficiency does a disservice to operational planners. The first portion of the analysis will examine the notion that the existing principles of war are timeless and will show that they in fact are not.

The Principles of War Are Not Timeless or Universally Accepted

For over half a century, U.S. military professionals have studied, and in many cases had to commit to memory, the principles of war and as a result the principles have evolved from the status of historically-derived truisms to being regarded as unquestionable dogma. However, the facts presented below do not support the notion that that principles of war are timeless or unchangeable.

First, as discussed in the preceding section on the origins of the principles of war, the principles as we know them today in U.S. doctrine date back less than a century and they have not been regarded as unassailable truths nor have they always been present in doctrine through the intervening years.

Second, the essential meaning of some principles has been twisted by time and interpretation such that we are left wondering how timeless the concept underlying a given

principle really is if it"s original meaning has been lost to history. Bernard Brodie, a renowned military scholar, highlighted one such example regarding the principle *economy of force* in a lecture delivered at the U.S. Army Command and General Staff College in 1957. Clausewitz"s discussion of *economy of force* in *On War* provides the classical meaning: "If a segment of one"s force is located where it is not sufficiently busy with the enemy, or if troops are on the march—that is, idle—while the enemy is fighting, then these forces are being managed uneconomically. In this sense they are being wasted, which is even worse than using them inappropriately."[26] Brodie asserted a common interpretation of the same principle was that "one should do a military job with the least forces necessary for that job."[27] The current doctrinal definition is: "The purpose of the economy of force is to allocate minimum essential combat power to secondary efforts."[28] In short, the classical description simply advises that all forces should be employed against the enemy while the current description focuses on minimizing secondary efforts. This may seem an argument of pure semantics but really it is not; the contemporary use of the word "economy" leads us to an understanding of the principle *economy of force* which is not the same as what was originally stated by military theorists such as Clausewitz.

Third, the specific principles listed in U.S. doctrine are not common across similar lists developed in other countries, even those countries with similar war fighting experiences. For example, France lists only three principles: concentration of effort, surprise, and liberty of action.[29] On this point Alger notes that "each country adopted notions of the principles of war best suited to its geography, political form, circumstance and national history.[30]

The salient points to be drawn from this element of the case are that military strategists should recognize the nine principles of war are in fact not very old as they are currently

defined and they are not universally accepted. The next logical question is whether the principles of war apply across all domains and across the range of military operations.

The Precedent for Tailored Principles

The creation of specialized lists of principles for specific categories of operations short of full-scale war is not without precedent. This is not surprising considering the principles of war as originally codified in U.S. Army doctrine and eventually adopted in joint doctrine were derived largely from the study of land warfare between "comparably armed and relatively equal foes."[31] Clearly there are categories of military operations which do not rise to the level of "war" and do not involve large scale, conventional land combat such as humanitarian assistance or counterinsurgency operations. These categories of operations have attributes which make the fundamental principles applicable to them different than those applicable to war. Several examples of alternative principles are elaborated below.

The "Other" Joint Principles. In the 1990s, *Joint Doctrine for Military Operations Other Than War* (MOOTW), JP 3-07, listed six *Principles of MOOTW* which included three traditional principles of war (objective, unity of effort, and security) and three principles unique to MOOTW (restraint, perseverance, and legitimacy.) Over time, the term MOOTW fell out of favor within U.S. doctrine and with the 2006 revision to JP 3-0, *Joint Operations,* the three unique MOOTW principles were relabeled as simply *other principles* and were combined with the nine traditional principles of war to form twelve *principles of joint operations*. JP 3-0's explanation of the origin and utility of these other principles is: "extensive experience in missions across the range of military operations has identified three additional principles that also may apply to joint operations."[32]

Principles of Counterinsurgency. The new doctrine document, *Counterinsurgency Operations*, JP 3-24, published in October of 2009 elaborates 13 principles of

counterinsurgency and states: "The principles of COIN are derived from the historical record and recent experience. These principles do not replace the principles of joint operations, but rather provide focus on how to successfully conduct COIN."[33]

Tenets of Air and Space Power. While the principles of counterinsurgency provide one example of additive principles specific to a category of operations, the *Tenets of Air and Space Power* as expressed in *Air Force Basic Doctrine*, AFDD 1, provide an example of the idea that the defined principles of war are not sufficient to truly express all of the fundamental truths derived from operations in domains other than the land domain. The fact these fundamental truths are defined as *tenets* as opposed to *principles* is immaterial considering *The American Heritage Dictionary* defines a *tenet* as an "opinion, doctrine, or principle held as being true by a person or especially by an organization." AFDD-1 provides the following explanation for the tenets: "They reflect not only the unique historical and doctrinal evolution of airpower, but also the specific current understanding of the nature of air and space power. The tenets of air and space power...complement the principles of war. While the principles of war provide general guidance on the application of military forces, the tenets provide more specific considerations for air and space forces."[34]

The case presented thus far has established: (1) the "timeless principles of war" are not that timeless or universally accepted, and (2) doctrine provides the precedent for developing tailored principles by domain or category of operations. Given these facts, the options expand and we are free to search for more descriptive ways to express the fundamental truths which should inform the prosecution of operations in cyberspace. The next and final section of the case for principles of cyberspace operations will illustrate how a new principle called *precision* would be more useful than *mass* for planning and executing cyberspace operations.

Precision versus Mass as a Principle of Cyberspace Operations

The Russian invasion of Georgia in 2008 is widely regarded as a landmark event in the history of armed conflict not because it was an invasion of one sovereign country by another, but because the invasion was preceded by a coordinated cyberspace attack.[35] The cyberspace attack was designed to deny access to, and in some cases take control of, critical Georgian government and civilian internet servers such as the websites of the President of Georgia, the Georgian Ministry of Foreign Affairs, and the Georgian Ministry of Defense.[36] A number of cyberspace attack tactics were used throughout the conflict in Georgia but the predominant method employed was the denial-of-service (DoS) attack. Broadly speaking DoS attacks are intended to make a computer resource unavailable to its intended users. There are numerous ways to conduct DoS attacks but in general they achieve their objective by either: (1) flooding and overwhelming the target system with communications requests; or (2) by causing the targeted system to reset through the use of malicious code designed to exploit vulnerabilities or flaws in the target system. Researchers who have studied the Georgia case have found evidence indicating both of these general tactics were employed.[37]

As a case study for examining the applicability of *mass* as a viable principle of war for cyberspace operations, we will now focus our attention on the style of DoS attack where a targeted system is flooded with communication requests with the intent to deny access to the system by its intended users. Often this type of DoS is conducted through a mechanism known as a *botnet.* Generally speaking a botnet is composed of hundreds or even thousands of *bots* which are individual computers which have covertly been brought into the service of the botnet through the introduction of malicious code (i.e., viruses, worms, etc.) The individual bots receive instructions through communications with a *command and control server* which is also a compromised host controlled by a cyberspace operator referred to as a

herder. To execute a DoS through a botnet, a herder will issue commands to their army of bots through the command and control server and the individual bots will begin attempting communications with the target system in the manner and at the time determined by the herder. Whether the bots attempt to induce errors in the targeted system or if they simply make repeated communication requests, the result is the same; the targeted system becomes unusable by its intended users.

Mass as a Principle of Cyberspace Operations. Having now established a real world instance where a cyberspace attack, specifically a botnet-based DoS attack, was successfully executed against Georgia, it is now appropriate to examine mass as a principle of war to determine its efficacy in capturing the fundamental nature of this method of warfare. JP 3-0 states "the purpose of mass is to concentrate the effects of combat power at the most advantageous place and time to produce decisive results." [38] If this definition of mass is used to frame our understanding of the botnet-based DoS attack scenario described previously, one could draw the conclusion that this style of cyberspace attack is a perfect application of mass in modern warfare. After all, a single herder using a single command and control server could instruct an army of bots to launch a coordinated attack against a targeted information system to produce a decisive result. However, upon further examination, a critical weakness is revealed in the assertion this scenario illustrates mass: the scenario just described is executed by a single herder (the only human in the scenario), not by an army of herders. To understand the relevance of this distinction, an examination of the origin of mass as a principle of war is warranted.

At their most basic within doctrine, the principles of war are presented as a simple list of single words or phrases without definition. Arguably this is the level of comprehension

many military personnel are able to retain reference the various principles of war. So, ignoring the doctrinal definition for a moment, what could mass mean to a military planner? Thinking of just the word "mass" many would intuitively think the principle would imply assembling or concentrating large numbers of troops or weapons systems. Given this, it is not at all surprising that this idea matches the origin of the principle in classical writings. Carl von Clausewitz did not describe a principle titled mass; however, he did discuss the concept of "concentration of forces in space." Specifically, his description was: "there is no higher and simpler law of strategy than that of *keeping one's forces concentrated.* No force should ever be detached from the main body unless the need is definite and *urgent.*"[39] Mass in its first appearance within U.S. doctrine by that name (as opposed to concentration) and with a complete definition appeared in the 1949 edition of Field Manual 100-5, *Field Service Regulations*: "Mass or the concentration of superior forces, on the ground, at sea, and in the air, at the decisive place and time, and their employment in a decisive direction, creates the conditions essential to victory."[40] Clearly the Army definition derived directly from Clausewitz"s earlier definition of concentration. As already indicated, this is not how mass is currently defined as a principle of war.

The current definition of mass means something strikingly different than it did when it was derived as a fundamental principle of war; as a matter of fact it now describes an idea of mass which is the exact opposite of how it was originally conceived. In other words, the classical definition referred explicitly to the concentration of forces while the current description in JP 3-0 states militaries should mass effects rather than concentrating their forces.[41] Why has this happened? It has happened because the ability to precisely apply devastating combat power through such things as precision weapons (e.g., "smart" bombs)

has made the concept of massing ones forces unnecessary and ill-advised. Evidently, rather than abandon the time honored principle of mass in favor of a new principle (or principles) which would make more sense for the way in which modern combat is conducted, the authors of our doctrine chose to mutate mass‟ definition. Why not abandon the term mass and derive something more appropriate as a principle of war for the modern age?

Precision as a Principle of Cyberspace Operations. Returning to the example of a botnet-based DoS cyberspace attack, the following statement can be used to summarize the method of attack: a single herder can precisely target an adversary‟s information system through the use of a distributed army of bots in a coordinated attack designed to deny the adversary freedom of action in cyberspace. While the reference to an "army of bots" indicates there will be a large numbers of bots involved in the attack, the critical aspect of this attack is the ability to *precisely target* an adversary‟s information system. From this statement, the principle *precision* can logically be derived.

Precision as a principle of cyberspace operations has applicability beyond the specific example DoS case presented. Thinking back to the attributes of cyberspace described earlier, it is easy to further justify the relevance of precision to cyberspace operations. Without precise application, offensive cyberspace operations have the potential to create effects beyond those intended. For example, the intentional release of malware into an adversary‟s system has the potential to spread outside of the targeted systems, perhaps even to allied nations. Additionally, blindly attacking a node in an adversary‟s cyberspace infrastructure could mean targeting an information technology asset physically located in an allied or neutral nation and owned by citizens of those same nations.

CONCLUSIONS AND RECOMMENDATION

Cyberspace is the newest officially recognized domain within which joint forces must conduct operations yet joint doctrine for the planning and execution of joint operations within cyberspace has not been published. All doctrine should be grounded on core principles and the intent of this paper was not to invalidate the existing principles of war; rather, it was to make the case that the existing principles of war alone are not sufficient to shape an operational cyberspace planner‟s thoughts on how best to conduct military operations in cyberspace. To support this assertion the case established a number of key points. First, the current principles of war are not as timeless and universal as they are often perceived to be. Second, there is a precedent within U.S. joint doctrine for establishing operation and domain-specific principles. Finally, an examination of the cyberspace attack on Georgia in 2008 illustrated how a principle called *precision* would be more useful for planning and executing cyberspace operations than the traditional principle *mass*.

Based on the information presented herein, it is clear there is a pressing need to develop comprehensive joint doctrine for cyberspace operations which should be grounded on principles of cyberspace operations. The analysis presented in this paper identified precision as one appropriate principle of cyberspace operations; however, there are certainly others. The identification of the total list of appropriate principles was beyond the scope of this paper; rather, the intent of this paper was to establish the fact that such a list should be developed. Therefore, it is recommended that the USCYBERCOM staff, in coordination with the broader joint doctrine development community, develop the tailored set of principles of cyberspace operations and associated joint doctrine to guide the planning and execution of joint operations in cyberspace with the ultimate objective of enabling U.S. forces to retain freedom of action in cyberspace while denying the same to our adversaries.

NOTES

[1] Chairman, Joint Chiefs of Staff, *National Military Strategy* (Washington, DC: CJCS, 2004), 18.

[2] DoD Office of Public Affairs, "U.S. Cyber Command Fact Sheet," http://www.defense.gov/home/features/2010/0410_cybersec/, 25 May 2010 (accessed 9 October 2010).

[3] Keith B, Alexander, "Warfighting in Cyberspace," *Joint Forces Quarterly* 46 (3rd Quarter, 2007): 59.

[4] Michael W. Wynne, "Flying and Fighting in Cyberspace," *Air & Space Power Journal* XXI, no. 1 (Spring 2007): 9.

[5] David B. Farmer, "Do the Principles of War Apply to Cyber War?" Monograph, Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 2010), 5, http://www.dtic.mil/ (accessed 6 September 2010).

[6] Ibid., 5.

[7] Sebastian M. Convertino, Lou Anne DeMattei, and Tammy M. Knierim, *Flying and Fighting in Cyberspace*, Maxwell Paper no. 40 (Maxwell Air Force Base, AL: Air University Press, July 2007), 75.

[8] Ibid., 39.

[9] U.S. Air Force, *Cyberspace Operations*, AFDD 3-12 (Washington, DC: Department of the Air Force, 15 July 2010), 16-17.

[10] AFDD 3-12, *Cyberspace Operations*, 16.

[11] Chairman, Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, 12 April 2001 as amended through 31 July 2010), 118.

[12] AFDD 3-12, *Cyberspace Operations*, 2.

[13] David M. Hollis, "USCYBERCOM: The need for a Combatant Command versus a Subunified Command," *Joint Forces Quarterly* 58 (3rd Quarter 2010): 49.

[14] AFDD 3-12, *Cyberspace Operations*, 10.

[15] Chairman, Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations,* (Washington, DC: CJCS, December 2006), 9-10, document is now declassified.

[16] William T. Lord, "USAF Cyberspace Command, To Fly and Fight in Cyberspace," *Strategic Studies Quarterly* 2, no. 3 (Fall 2008): 7.

[17] JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 118.

[18] Information Operations are defined as: "The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own." JP 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 225.

[19] Ibid., 225.

[20] Keith B. Alexander, "Testimony," House, *Statement of General Keith B. Alexander Commander United States Cyber Command Before the House Committee on Armed Services*, 111th Cong., 2nd sess., 23 September 2010, 4.

[21] Chairman, Joint Chiefs of Staff, *Doctrine for the Armed Forces of the United States,* JP 1 (Washington, DC: CJCS, 02 May 2007 incorporating change 1 20 March 2009), I-1.

[22] JP 1, *Doctrine for the Armed Forces of the United States*, I-2.

[23] John I. Alger, *The Quest for Victory*, Contributions in Military History, no. 30 (Westport, CT: Greenwood Press, 1982), 14.

[24] Ibid., 16.

[25] Ibid., xxi-xxii.

[26] Carl von Clausewitz, *On War,* ed. and trans. Michael Howard and Peter Paret (Princeton NJ: Princeton University Press, 1976), 213.

[27] Bernard Brodie, "The Worth of Principles of War," RAND Report P-1092 (Santa Monica, CA: RAND Corporation, 21 May 1957), 11.

[28] Chairman, Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington, DC: CJCS, 22 March 2010 with change 2), A-2.

[29] Joint Forces Staff College, *The Joint Staff Officer's Guide 2000*, (Norfolk, VA: Joint Forces Staff College, 2000), D-2.

[30] Grant T. Hammond, "The U.S. Air Force and the American Way of War," in *Rethinking the Principles of War*, ed. by Anthony D. Mc Ivor (Annapolis, MD: Naval Institute Press, 2005), 116.

[31] Alger, *The Quest for Victory*, xxiii.

[32] JP 3-0, *Joint Operations*, II-1.

[33] Chairman, Joint Chiefs of Staff, *Counterinsurgency Operations*, Joint Publication JP 3-24 (Washington, DC: CJCS, 5 October 2009), xv.

[34] U.S. Air Force, *Air Force Basic Doctrine,* AFDD 1 (Washington, DC: Department of the Air Force, 17 November 2003), 27.

[35] Georgia Update, "Russian Cyberwar on Georgia," 10 November 2008, http://georgiaupdate.gov.ge/en/facts (accessed 22 October 2010), 2.

[36] Ibid., 5.

[37] Jeff Carr, "Russia/Georgia Cyber War – Findings and Analysis," Project Grey Goose: Phase I Report, 17 October 2008, http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (accessed 23 October 2010), 9-11.

[38] JP 3-0, *Joint Operations*, A-1.

[39] Clausewitz, *On War,* 204.

[40] Alger, *The Quest for Victory*, 254-255.

[41] JP 3-0, *Joint Operations*, A-1.

BIBLIOGRAPHY

Alexander, Keith B. "Warfighting in Cyberspace." *Joint Forces Quarterly* 46 (3rd Quarter, 2007): 58-61.

Alger, John I. *The Quest for Victory*. Contributions in Military History, no. 30. Westport, CT: Greenwood Press, 1982.

Andrues, Wesley R. "What U.S. Cyber Command Must Do." *Joint Forces Quarterly* 59 (4th Quarter 2010): 115-120.

Brodie, Bernard. "The Worth of Principles of War." RAND Report P-1092. Santa Monica, CA: RAND Corporation, 21 May 1957.

Bronaugh, Casey. "„Other" Principles of War." Research paper, Newport, RI: U.S. Naval War College, Joint Military Operations Department, 3 May 2010.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Pater Paret. Princeton, NJ: Princeton University Press, 1976.

Convertino, Sebastian M., Lou Anne DeMattei, and Tammy M. Knierim. *Flying and Fighting in Cyberspace*, Maxwell Paper no. 40. Maxwell Air Force Base, AL: Air University Press, July 2007.

Crowell, Richard M. "NWC 2021: War in the Information Age: A Primer for Cyberspace Operations in 21st Century Warfare." Newport, RI: U.S. Naval War College Joint Military Operations Department, 2009.

Echevarria, Antulio J. "Principles of War or Principles of Battle." In *Rethinking the Principles of War*, edited by Anthony D. Mc Ivor. Annapolis, MD: Naval Institute Press, 2005.

Farmer, David B. "Do the Principles of War Apply to Cyber War?" Monograph, Fort Leavenworth, KS: Army Command and General Staff College, School of Advanced Military Studies, May 2010. http://www.dtic.mil/ (accessed 6 September 2010). Available as Defense Technical Information Center Report (DTIC) ADA522972.

Georgia Update. "Russian Cyberwar on Georgia." 10 November 2008. http://georgiaupdate.gov.ge/en/facts (accessed 22 October 2010).

Hammond, Grant T. "The U.S. Air Force and the American Way of War." In *Rethinking the Principles of War*, edited by Anthony D. Mc Ivor. Annapolis, MD: Naval Institute Press, 2005.

Hollis, David M. "USCYBERCOM: The need for a Combatant Command versus a Subunified Command." *Joint Forces Quarterly* 58 (3rd Quarter 2010): 48-53.

Johnsen, William T., Douglas V. Johnson II, James O. Kievit, Douglas C. Lovelace, Jr., and Steven Metz. "The Principles of War in the 21st Century: Strategic Considerations." Monograph, Carlisle Barracks, PA: Strategic Studies Institute, United States Army War College, 1995.

Joint Forces Staff College. *The Joint Staff Officer's Guide 2000.* Norfolk, VA: Joint Forces Staff College, 2000.

Korns, Stephen W. "Cyber Operations: The New Balance." *Joint Forces Quarterly* 54 (3rd Quarter 2009): 97-102.

Leonhard, Robert R. *The Principles of War for the Information Age*. Novato, CA: Presidio Press, 1998.

Lord, William T. "USAF Cyberspace Command, To Fly and Fight in Cyberspace." *Strategic Studies Quarterly* 2, no. 3 (Fall 2008): 5-17.

Paul, Richard, and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. Dillon Beach, CA: The Foundation for Critical Thinking, 2006.

Carr, Jeff. "Russia/Georgia Cyber War – Findings and Analysis." Project Grey Goose: Phase I Report. 17 October 2008. http://www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report (accessed 23 October 2010).

Tomes, Robert R. "Rethinking Operational Art." In *Rethinking the Principles of War*, edited by Anthony D. Mc Ivor. Annapolis, MD: Naval Institute Press, 2005.

U.S. Air Force. *Air Force Basic Doctrine.* Air Force Doctrine Document (AFDD) 1. Washington, DC: Department of the Air Force, 17 November 2003.

U.S. Air Force. *Cyberspace Operations*, AFDD 3-12. Washington, DC: Department of the Air Force, 15 July 2010.

U.S. Congress. House. *Statement of General Keith B. Alexander Commander United States Cyber Command Before the House Committee on Armed Services*. 111th Cong., 2nd sess., 23 September 2010.

U.S. Department of Defense Office of Public Affairs, "U.S. Cyber Command Fact Sheet." U.S. Department of Defense Office of Public Affairs. http://www.defense.gov/home/features/2010/0410_cybersec/, 25 May 2010 (accessed 9 October 2010).

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Doctrine for the Armed Forces of the United States.* Joint Publication (JP) 1. Washington, DC: CJCS, 02 May 2007 incorporating change 1 20 March 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms.* JP 1-02. Washington, DC: CJCS, 12 April 2001 as amended through 31 July 2010.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operations.* Joint Publication (JP) 3-0. Washington, DC: CJCS, 22 March 2010 with change 2.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Information Operations*. JP 3-13. Washington, DC: CJCS, 13 February 2006.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Counterinsurgency Operations.* JP 3-24. Washington, DC: CJCS, 5 October 2009.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy.* Washington, DC: CJCS, 2004.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *National Military Strategy for Cyberspace Operations.* Washington, DC: CJCS, December 2006. Document is now declassified.

U.S. Office of the Secretary of Defense. *The National Defense Strategy of the United States of America.* Washington, DC: DOD, March 2005.

U.S. President. *Cyberspace Policy Review.* Washington, DC: The White House, May 2009.

U.S. President. *The National Security Strategy of the United States of America*. Washington, DC: The White House, May 2010.

U.S. President. *The National Strategy to Secure Cyberspace*. Washington, DC: The White House, May 2010.

Wynne, Michael W. "Flying and Fighting in Cyberspace." *Air & Space Power Journal* XXI, no. 1 (Spring 2007) 5-9.