Strategy Research Project

CYBERSPACE DOMAIN: A WARFIGHTING SUBSTANTIATED OPERATIONAL ENVIRONMENT IMPERATIVE

BY

COLONEL OLEN L. KELLEY
United States Army

USAWC CLASS OF 2008

U.S. Army War College, Carlisle Barracks, PA 17013-5050

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
15 MAR 2008	**Strategy Research Project**	**00-00-2007 to 00-00-2008**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Olen Kelley	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
U.S. Army War College ,122 Forbes Ave.,Carlisle,PA,17013-5220	
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
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
See attached

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**34**	

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

USAWC STRATEGY RESEARCH PROJECT

CYBERSPACE DOMAIN: A WARFIGHTING SUBSTANTIATED OPERATIONAL ENVIRONMENT IMPERATIVE

by

Colonel Olen L. Kelley
United States Army

Colonel David J. Smith
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

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

ABSTRACT

AUTHOR: Colonel Olen L. Kelley

TITLE: Cyberspace Domain: A Warfighting Substantiated Operational Environment Imperative

FORMAT: Strategy Research Project

DATE: 25 March 2008 WORD COUNT: 6,332 PAGES: 34

KEY TERMS: Information Superiority, Information Operations, Command and Control, Communications

CLASSIFICATION: Unclassified

The DOD has expended considerable effort in a “piece meal” strategy that updates information related doctrine based on new technology instead of developing a comprehensive and convergent cyberspace strategy. The effort to define and structure cyberspace or information is well intentioned, but currently fruitless. Additionally, lexicon issues have been problematic to the doctrinal communities in developing cyberspace as a battlespace.

Domains are where the military provides doctrine, training, and the necessities for war. This paper argues that clear consensus is needed to establish a new operational “cyberspace domain” where Joint Force Commander’s conduct war “as an act of force to compel our enemy to do our will.” It further argues that advancing the proposed National Military Strategy for Cyberspace Operations’ cyberspace domain definition clarifies information operation’s roles and functions, thereby enabling, gaining and maintaining information superiority.

CYBERSPACE DOMAIN: A WARFIGHTING SUBSTANTIATED OPERATIONAL ENVIRONMENT IMPERATIVE

The real object of having an Army is to provide for war.

—Secretary of War Elihu Root

The *raison d'etre* for a military force is to fight and win their nation's wars. It is for this singular purpose that each of the United States (U.S.) military departments organizes, mans, equips, and trains its forces. Aligned with this national purpose, each service acts in the primacy of an operational environment. The Air Force is organized to effect aerospace superiority, the Navy functions to reign supreme on the seas, and the Army dominates the land across the full range of military operations.[1] The Army embodies this purpose in its mission,[2] and it's embedded into each soldier's ethos. A domain is a "territory over which rule or control is exercised".[3] These operational environments are warfighting domains which represent physical expressions where military operations are conducted; where Joint Force Commanders (JFC) contest the enemy for dominance. Though each service shares time and space in every combat domain, each service jealously covets their respective primary warfighting domain. This alignment with service and operational environments is clearly defined and accepted in all areas but one, the cyberspace domain.

In 2001, Joint Publication (JP) 3-0 identified five warfighting domains.[4] The document contained the commonly accepted four operational environments, but added a new domain, which the authors termed *information*. This landmark inclusion started an intense debate within the Joint community. Previous clarity on the commonly accepted operational environment's roles and functions became blurred. Those who advocated information as a warfighting domain advanced its common understanding, yet could not

reach doctrinal consensus due to the many diverse points of view and equities. Discussions about how to describe, organize, and use the U.S.'s information capabilities to support the Department of Defense (DOD) strategic and operational objectives, and national security goals remain contentious and ambiguous.

This inability to develop consensus led to the re-characterization of information in the current JP 3-0, *Joint Operations*, from a warfighting domain to an "environment." However, this change did not resolve the fundamental issue and the information domain debate continues unabated. The recently published National Military Strategy for Cyberspace Operations (NMS-CO) again officially codified its understanding of "information," now defined as cyberspace, as a warfighting domain. It acknowledges the JP 3-0 information domain change to environment, but emphasizes that "treating cyberspace as a domain establishes a foundation to understand and define its place in military operations."[5]

The DOD has expended considerable effort in a "piece meal" strategy that updates information related doctrine based on new technology instead of developing a comprehensive and convergent cyberspace strategy. The effort to define and structure cyberspace or information is well intentioned, but currently fruitless. Additionally, lexicon issues have been problematic to the doctrinal communities in developing cyberspace as a battlespace.[6]

It is in a domain that the military "is to provide for war."[7] This paper argues that a clear consensus is needed to establish a "cyberspace domain" where JFC's conduct war "as an act of force to compel our enemy to do our will."[8] It further argues that

advancing the proposed NMS-CO's cyberspace domain definition clarifies information operation's roles and functions, thereby enabling information superiority.[9]

The Military Significance of Information

Military information exists for two purposes; situational awareness and decision-making. These form the foundation of command and control (C2) and underpin the need to establish a cyberspace domain. Effective command and control is contingent on the reliable, relevant transfer of information that is clearly understood by both the initiator of the information and the actor receiving the information. From this mutual understanding action is taken or prescribed. Communications can be impaired or defeated by space, time, or the enemy, impeding the process. Units distanced from the commander experience this problem and can miss or receive information too late to effect the proper action. The enemy also has the means to amplify the problem by taking action to stop friendly information flow. To protect friendly information flow or deny it to the enemy is an aim for the military commander. History is replete with examples of communication innovations and battle tactics to overcome this problem. The battles that rage in cyberspace are centered on this.

The dramatic improvement in communications technology have reduced these limitations and facilitated the symbiotic relationship between information systems innovations and military applications. The telecommunications infrastructure and the information that reside on it are important components of national security. The historical development and innovation of communications and information infrastructures is closely aligned with military purposes.[10] This relationship has many precedents. In fact, during World War II, President Roosevelt federalized the U.S.

telecommunications network and managed it through the Board of War Communications.[11]

Leading edge technologies, such as the solid state transistor and digital communications switches were developed by commercial companies for military use. This relationship intensified with the development of the computer. The armed forces quickly realized the tremendous potential computer networks brought to military applications. Suddenly, information could be transferred from one decision maker to another asynchronously with great surety and clarity. This information flow led to information systems that ameliorated situational awareness and decision-making. Actors, both friendly and belligerent, recognized that this capability could be exploited and used, it could be melded with weapons systems, and perhaps most importantly, it could be exploited as a weapon.

In 1991, the U.S. and coalition forces penetrated defensive zones, disrupted Iraqi command and control and severed their lines of communications, which led to the Persian Gulf War being referred to the first information war.[12] This reference is a misnomer. The struggle to dominate the enemy through the use of information and knowledge is not new. The ability to gather intelligence and facilitate command and control while denying the enemy their ability to do the same is an extension of existing principles of war and previous military efforts. In fact, the genesis of electronic combat originated in WWII and matured as an element of warfare during the Viet Nam war.[13] The certainty of which coalition forces achieved such dominance in every military information activity led many to believe that the Gulf War "differed fundamentally from any previous conflict" in that "the outcome turned as much on superior management of

knowledge as . . . upon performances of people or weapons."[14] Whether this is valid or not, no one can dispute that the information explosion and the rapidity of communication systems that could, store, modify, and disseminate it were impacting military operations. Throughout the 1990's and into the 2000's the Department of Defense grappled doctrinally, and with great difficulty with what all this meant.

Doctrine Responds to a New Type of Warfare

The genesis of information warfare doctrine transpired throughout the 1990s. Three important precepts emerged during this period which still underpins today's cyberspace strategies. In 1992, the DOD produced a classified directive TS3600.1*, "Information Warfare."* [15] This document is one of the earliest official attempts to define a framework for information warfare. It was instrumental in that it aligned warfare with information and in the process prescribed a new battlespace. Other doctrinal efforts quickly followed. In 1996, the Air Force attempted to refine its doctrinal construct in a white paper, also called, *Information Warfare.*[16] Doctrine Document 2-5 (DD 2-5), *Information Operations* quickly followed and codified the Air Force's information warfare vision. One of DD 2-5's main tenets asserts that information warfare has both, an offensive and defensive dimension. In the interim the Army developed its own information warfare doctrine, also in the form of *Information Operations* (IO). Army doctrine brought form to IO and defined it as the means for "gaining and maintaining the information the warfighter requires to fight and win, while denying that same information to the enemy," in effect achieving information dominance.[17]

This doctrinal apex occurred when the Joint Chiefs of Staff (JCS) published *Joint Vision (JV) 2010* establishing information superiority as the critical enabling element for

21st century warfare. It went on to describe that superiority in the information domain is enabled by C2, fused all source intelligence, dominant battlespace awareness, and offensive and defensive information warfare.[18] The JCS's current vision, *Joint Vision 2020* envisions that the information domain is a battlespace in which the U.S. seeks dominance or superiority. *JV 2020* implores the doctrine community that the "pace of change in the information environment dictate that we expand this view and explore broader information operations strategies and concepts."[19] Though, the Joint Vision construct has fallen out of vogue, it set the course for future strategies and current doctrine to address the need for information superiority. Joint doctrine describes this as "the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary the ability to do the same."[20]

Today's information and cyberspace warfare doctrine consistently combines the three key tenets postulated during its doctrinal infancy. Information doctrine consists of offensive and defensive military activities, similar to those executed in air, land, sea, and space domains, which are designed to influence an adversary.[21] These information operations are enabled through achieving mission information superiority. IO core activities are Psychological Operations (PSYOP), Military Deception (MILDEC), Operations Security (OPSEC), Electronic Warfare (EW), and Computer Network Operations (CNO).[22] Information superiority is the end (objective) of information operations, while the capabilities are the means to achieve the end.

Doctrine is not meant to be stagnant and slowly evolves as the potential of new technology is realized or different aspects of threat capabilities are recognized. Apart

from doctrine, strategies and visions are more amenable and open to new ideas. The Joint community now recognizes that non-kinetic (information) or non-lethal weapon systems can create desired effects in prosecution of a task or mission. Joint Publications[23] insert information operations into Joint Functions that are offensive (Fires) and defensive (Protection) functions, as well as, the traditional enabler of command and control in Joint operations and forces.[24] The Force Application Joint Functional Concept[25] defines engagement as either lethal or non-lethal (information operations) to create the desired effect. According to this concept this type of engagement is part of force application that is conducted through the cyber domain.[26] The NetCentric Environment Joint Functional Concept outlines a strategy that separates and synergizes knowledge and technical areas in order to share information, protect, and act on information.[27] Unfortunately, current doctrine is based on existing capabilities and not on future strategies and concepts that may be implemented sometime in the future.[28] An impetus for doctrine to quickly assimilate new concepts lay in the need to develop a comprehensive information strategy to counter the many exigent existing and potential future threats.

Challenges and Threats to Information Superiority

The U.S.'s reliance on information systems has created a target rich environment for any adversary. The vulnerability of the U.S.'s critical infrastructure through cyberspace is well documented, and the sophistication of cyber attacks is increasing. Cyber attacks oriented on electrical grids and financial institutions can erode public confidence and create devastating long term effects on a state's economy. Conservative reports indicate that 20 to 30 countries are developing or currently

possess cyber attack capabilities.[29] Malicious attacks on DOD computers have steadily increased. In 2001 alone 40,000 such attacks were documented. The most widely known cyber warfare initiative and capability resides in China. China has been conducting cyber warfare exercises since 1997 and operating an information warfare military unit since 2000.[30] Security experts state that Chinese hackers are mapping the U.S.'s critical infrastructure with a primary focus on financial networks.[31]

Unrestricted Warfare, written by two Chinese military officers, proposes an asymmetric warfare strategy that employs all means and tactics to defeat a nation with a superior military force, like the U.S. [32] One of the asymmetric tactics presented in this book is to attack information networks that are critical to managing communications, transportation, and finances. Attacks that disable information networks can easily hamstring a large metropolis that is dependent on them for daily or business activities. The authors state that "…in the information age, the influence exerted by a nuclear bomb is perhaps less than the influence exerted by a hacker."[33] China has set its sights on developing this "cyber craft" and sees it as a critical warfighting capability. Evidence of this occurred in 2003, when the Chinese launched a series of coordinated attacks on U.S. computer systems, code named Titan Rain, by the U.S. government. An attack took less than 30 minutes leaving behind an almost undetectable means to reenter a computer. Later, it was determined that these attacks emanated from three Chinese routers in the province of Guangdong.[34] These efforts demonstrate Chinese resolve to shape the battlefield of tomorrow through cyberspace today.

Non-state actors, like Al Qaeda, clearly have the means to operate in cyberspace. Though terrorists groups generally employ physical attacks to compel world attention to

their cause, there is concern that cyberspace offers new tactics for these groups to coerce people or an even state. Alluding to the use of asymmetric attacks, Osama Bin Laden asserted that, “It is very important to concentrate on hitting the U.S. economy through all possible means.”[35] Shortly after in August 2003, Al Qaeda claimed responsibility for the blackout that blanketed the Northeast. Though later analysis found this not to be true, the fact that Al Qaeda made the claim demonstrated that attacks on American infrastructure and economy through cyberspace is a “possible means.” Sheik Omar Bakri Muhammad, leader of al-Muhajiron, a London based Islamist organization, until its disbandment in 2004, spoke definitely on the matter of Al Qaeda attacking through cyberspace. The Sheik cautions, “I would advise those who doubt Al Qaeda’s interest in cyber weapons to take Osama Bin Laden very seriously.”[36] It seems that Al Qaeda is very interested in developing the tools and means to reinforce their rhetoric. American intelligence discovered a hideout in Pakistan that was being used to train hackers to attack computer networks of nuclear plants and power grids.[37] Non-state actors lack the resources or sophistication a nation can bring to bear in cyberspace, but retain the intention and the capability to battle within it.

These Drivers Contest Current U.S. Joint Information Doctrine

This broad review of the civil-military use of information technology, the development of information warfare concepts, and the potential threat to America’s critical infrastructure through telecommunication and information networks highlights two essential points. Foremost, a clear danger exists. The development of human capital in using information and manipulating information systems is a primary pillar of asymmetric warfare. This capability and the acuity to employ malicious intent reside in

both, state and non-state antagonists. The proliferation of communications systems technology and the means to manipulate information has increased the capacity of states and transnational non-state actors to challenge U.S. information superiority.

Vulnerabilities within a state's information networks provide a weaker adversary the means to indirectly create national instability in an effort to increase their power and influence. The cardinal means to attack a state's weakness is through and in cyberspace. Cyber attacks on legal, financial, information through the cyber systems that enable them can be equally, if not more, disruptive than through the use of kinetic weapons.

The ability to maintain national will, to ensure security of vital interests, and to the craft effective diplomacy is hampered by an adversary's adroit use of information. Complicating this is enemy's capacity to evade accountability for information systems attacks and their ability to manipulate or abrogate public perception on foreign policy. It is the current and potential adversary that frames the requirement for a cyberspace domain and an effective information operations doctrine.

The second point is that the relationship between information systems, and command and control is inextricable linked and is more integral today than in any time in military history. However, undermining this is the fact that doctrine has not kept pace with this relationship. Information and cyberspace domain strategies, and the development of information operations doctrine are disparate and often divergent. The terms information environment, information operations, and cyberspace domain are often used interchangeably. Adding to the confusion is that the meanings conveyed with these different terms are inconsistent and often at odds with each other.

Compounding this problem is that information and cyberspace strategies, and doctrinal ideas and structure are found part and parcel in assorted doctrinal manuals, functional and integrating concepts throughout the joint community.[38] These issues continue to hinder progress in establishing the right conditions to maintain information superiority. A singular approach is needed with a clear endstate in mind. Currently, one does not exist. This current imbroglio is reflected by the different approaches that each service is taking to achieve information superiority for the warfighter.

DOD's Divergent Employment of Information Doctrine

U.S. Strategic Command (USSTRATCOM). The responsibility for information operations, network warfare and defense of the Global Information Grid (GIG) is USSTRATCOM. USSTRATCOM established three separate Joint Functional Component Commands (JFCC) to accomplish these information missions. These JFCCs found their genesis in Unified Command Plan 2002 (Change 2) with the intent to assure global information superiority.[39] At the strategic level, these JFCCs form a strategic triad in support of the U.S.'s cyber warfare strategy. Joint Task Force Global Network Operations (JTF-GNO) is responsible for the Global Information Grid, JFCC - Network Warfare (JFCC-NW) is responsible for coordinating DOD offensive computer network operations. Finally, the Joint Information Operations Warfare Center (JIOWC) is responsible for the integration of IO into military plans and operations. According to the former USSTRATCOM Commander, General James Cartwright, this triad construct is a "passive, disjointed approach that undermines the military's cyberspace operations."[40] The construct General Cartwright mentions was founded on computer terminal defense and thereafter pieced together. This horizontal approach to cyber warfare is reactive

and a coordinated response too often delayed to generate the desired outcome. The solution proposed by General Cartwright is to move DOD “away from a network defense-oriented architecture” and integrate cyber offensive and defensive capabilities.[41] Under this current, disjointed strategic approach the services are taking their own independent steps to conduct cyberspace operations at the operational and tactical levels.

NAVY. In 2002, the Navy stood up the Naval Network Warfare Command to be its central operational authority for space, network management and information operations. In 2005, this consolidation was completed with the integration of the information operations organization, formerly conducted by the Navy’s Naval Security Group Command. The Navy’s actions consolidate communications and information systems activities with the functions that “operationalize” the information that flows through these systems into a singular organization. This approach aligns disparate organizations into a singular organization that can vertically leverage all the capabilities to a common aim. However, a fallacy in this approach is that it removes critical aspects of Information Operations (IO), primarily those activities that focus on influencing the adversary’s decision-making from the warfighter. A main component of IO uses information to influence the behavior or decision process of a selected adversary or targeted audience. The IO core and related activities that support this aim are integral to commander’s applying the information element of combat power.[42] Integration of this capability from this new organization to a commander is a process that is necessary to achieve naval operational success.

ARMY. The Army is taking a wait and see attitude on cyberspace as an operational domain. In this regard, the Army is studying the other services and asking, "Are there any ideas that the Army should be adopting?"[43] The Army is viewing with interest the recent Air Force initiatives in cyberspace. It took notice of the Air Force's change to its mission statement to include cyberspace as domain, commenting that this is a "development worthy of our assessment."[44]

The Army has invested most of its efforts in developing IO as the centerpiece of their cyber warfare strategy. Currently, the Army is holding steady that IO is the best means to gain and maintain information superiority.[45] Once a commander achieves information superiority, he can shape the information environment and set the conditions for the other elements of combat power. The concept states that there are four interdependent activities to achieve this type of dominance:

- Army information tasks – tasks used to shape the operational environment.
- Intelligence, surveillance, and reconnaissance – activities conducted to develop knowledge about the operational environment.
- Knowledge management – the art of using information to increase knowledge.
- Information management – the science of using information systems.[46]

The Army has taken a decentralized approach that differs from the Navy's. There are several separate organizations responsible for various functions of information operations and telecommunications systems. The Army's current position is that cyberspace is part of IO and that cyberspace resides in the information environment.[47]

This position seems doctrinally at odds with itself. The confusion starts when "soft power" information activities, such as psychological operations (PSYOP), are said to

contribute to an operational advantage through the uninterrupted flow of information. The unimpeded ability to move information throughout the battlefield can only be achieved by dominating the cyberspace domain. The “soft power” information activities that are designed to influence the adversary’s decision-making are a static capability until processed, collected, and/or disseminated. The ability to process, collect, and disseminate information is a condition of operating with information superiority. Information superiority is only achieved once information processes, systems and technologies function without enemy, or natural interference. This information dominance allows the commander to direct “soft power” information to a target audience or an adversary.

AIR FORCE. On Dec. 7, 2005, cyberspace became an official Air Force warfighting domain after Secretary of the Air Force, Michael W. Wynne, and Chief of Staff of the Air Force, Gen. T. Michael Moseley, announced the need to “deliver sovereign options for the defense of the United States of America and its global interests -- to fly and fight in air, space, and cyberspace."[48] In 2007, the Air Force announced it would create the Cyber Command, to be headquartered at the 8th Air Force at Barksdale Air Force Base, Louisiana, and is expected to be fully operational in 2008.[49] The Cyber command plans to move beyond the idea of cyberspace “as network operations, information operations or use of the internet as an enabler for military operations in physical domains.”[50] The three mission areas for cyberspace operations include defending cyber systems by preventing an enemy from disrupting communications. The second involves gathering intelligence on adversaries’ cyber

activities. The third and most controversial aspect of cyberwarfare contemplates the possibility of U.S. forces conducting offensive computer network attack.

The command intends to integrate the Air Force's functions for command and control, electronic warfare, network warfare, intelligence, surveillance and reconnaissance (ISR), and apply them across the continuum of warfare. On request, the command will support civilian authorities.[51] The Air Force is focusing on securing information superiority to enable information operations. This is a means to further operationalize information by ensuring the military has the freedom to operate freely in the cyberspace domain. Future efforts for the Air Force are predicated on the realization that "Cyberspace is more than networks. It includes the entire electromagnetic spectrum (EMS)."[52]

Air Force efforts are still in their infancy. The possibility to define their newest domain is ripe for innovation. The inclusion of communication/information platforms that use the EMS is a key concept in defining the cyberspace domain. The offensive and defensive cyberspace tenets are the hard power functions[53] removed from IO that ensure the ability to protect, defend, and move information while preventing the enemy the same privilege. This specifies the capabilities needed to affect or defend communication networks and information systems.

The addition of ISR into the cyberspace domain is a unique step. ISR refers to the sets of collection and processing systems, and associated operations, involved in acquiring and analyzing information. Cyberspace activities that ensure freedom of action to conduct intelligence operations nests with the domain construct. However,

activities in acquiring intelligence and associated analysis functions maybe better utilized and developed elsewhere.

There is a wide range of responses within the different services in how to secure and maintain information superiority, and to the benefits of establishing a cyberspace domain to achieve that superiority. This analysis of service efforts to operationalize information highlights a third key point. Cyberspace unlike other domains does not have a predominant service stakeholder who drives doctrine. Therefore, doctrinal tenets are inconsistently interpreted and applied by the services. It has been demonstrated that the establishment of a domain and a primary driver can focus doctrine on how to best achieve dominance in it. For example, the Army's intent is to dominate the land domain through the doctrinal application of maneuver and fires. The same concentration can be applied to a cyberspace domain and the same doctrinal clarity established.

The Evolution of the Information Environment to a Warfighting Domain

As discussed previously, the critical doctrinal point of contention is whether information is a "domain" or an "environment." The *information environment* construct was first proposed in the Joint publications under the (DOD) Command and Control Research Program (CCRP). It is defined as the aggregate of individuals, organizations and systems that collect, process, disseminate, or act on information.[54] Now we see its fruition in the recently published Joint Publication 3-13, *Information Operations*. The information environment is comprised of three distinct, separate but interrelated dimensions – physical, information, and cognitive (Figure 1).[55] The *physical dimension* "is where the physical elements of information systems and networks reside" and where military maneuver and combat operations occur.[56] Elements within this dimension are

easier to measure and define than other dimensions. Physical dimension attributes directly correlate with those associated with air, land, sea, and space domains. It is the place where the military seeks to influence, control or dominate resides. It is characterized as the ground truth.[57]

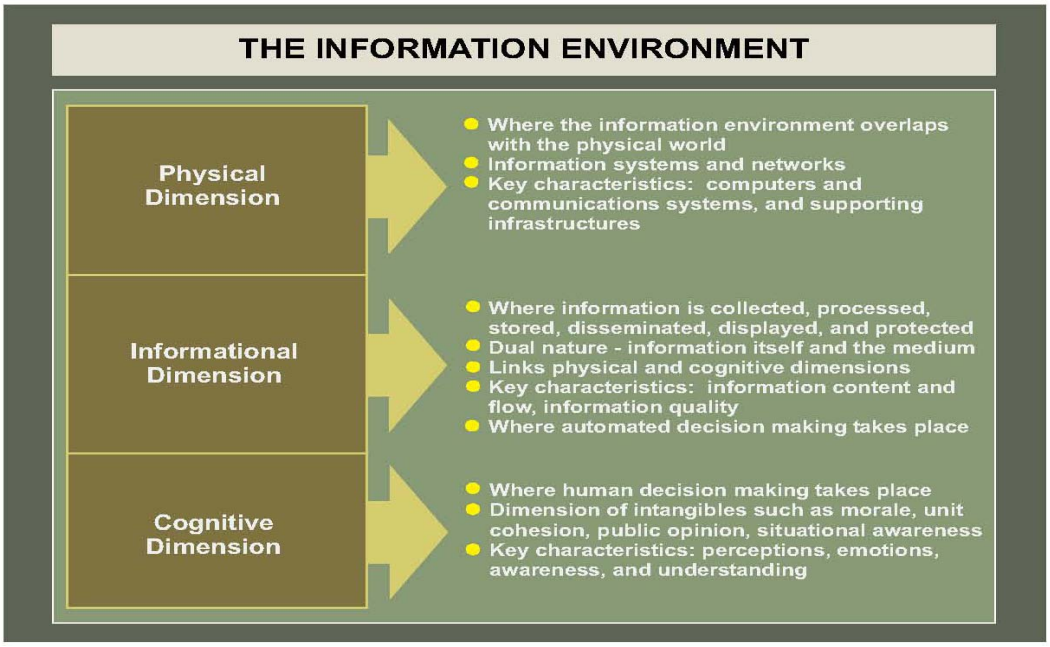

Figure 1. The Information Environment (Source JP 3-13)

The *information dimension* represents the information itself; where information is created, manipulated, and shared.[58] This dimension is where "information lives."[59] It is where the command and control of modern military forces is communicated and where commander's intent is conveyed,[60]protected, and defended to enable a force to generate combat power.[61] The information dimension links the physical and cognitive dimensions. Knowledge management is the process that connects the cognitive dimension with the information dimensions through the physical dimension. It is a conceptual abstract based in part on theory, thus more difficult to measure.

The *cognitive dimension* is also abstract and theoretical. This dimension resides in the mind of the commander, as the decision maker, and the intended target. The cognitive dimension is where the decision process takes place and where many battles and wars are actually won or lost.[62] This is the realm of intangibles: public opinion, situational awareness, leadership, experience unit cohesion, and morale.[63] The cognitive dimension wages battle in and between the participant's minds, and as such is the most important of the three dimensions.

A compromised position that deserves serious consideration is found in the recently published National Military Strategy for Cyberspace Operations (NMS-CO). It defines cyberspace as, "A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructure."[64] This definition accomplishes two determinative things. The first is that it establishes cyberspace as a warfighting domain. It is a domain that has characteristics similar to traditional warfighting domains. The definition makes it a physical domain by establishing physical boundaries to the domain in the form of the electromagnetic spectrum (EMS). It encompasses all things of, relating to, or within the EMS, including all cyberspace related activities, infrastructures, people, and telecommunications and information systems that comprises "electronics" as the means or tools to conduct cyber warfare.

The second key aspect of this definition is that it separates "information" from cyberspace. Cyberspace therefore is discrete from the information that is stored, modified or exchanged through the network. It goes on to characterize that this domain

forms the foundation of the information environment, and performs as an enabler of information.[65]

As noted earlier, the NMS-CO prescribes a new domain (cyberspace) that is distinct from the information that may reside or communicated through it. At first look this definition contradicts the information dimensions definition. A closer analysis of both definitions shows that is only partially true. Assuming cyberspace is doctrinal accepted as a domain then two modifications to the information dimension concept, in JP 3-13, are necessary. First, the cyberspace domain subsumes all the functions and activities in the physical dimension of the information environment, and the manipulating and sharing of information in the information dimension. Second, the physical dimension is sundered as part of the information environment, and only the creating of information in the information dimension and cognitive dimension remain*. In other words, the information environment becomes the aggregate of individuals and organizational processes that create and act on information.* Whereby, the cyberspace domain becomes the contested territory (electromagnetic spectrum) over which kinetic and non-kinetic warfighting activities are conducted to allow the flow of information and deny the enemy the same, in essence establishing information superiority.

Substantiating Cyberspace's Credentials as a Domain

Domains infer that the physical dimensions of land, sea, air, and space are a battle space defined by physical properties in time and space; a place with real political, economic, and military value, where nations and actors seek to dominate their adversaries. The military conducts offensive and defensive operations in these domains for the purposes of achieving U.S. national security objectives. Warfighting domains

focus their collective energy on this endstate. All cyberwar activities and associated doctrinal development should focus on the same endstate. The following is a doctrinal list of extracted commonly accepted domain characteristics and activities:[66]

1. It is a physical area bounded by the laws of physics.

2. Joint Force Commanders seek to gain the initiative and maintain control; domain superiority permits the conduct of operations without effective opposition.

3. Military maneuver & operations occur to place the enemy at a disadvantage.

4. Specialized equipment and personnel training are a prerequisite to effectively battle within a domain.

5. Military organizations and command structures are proscriptive and exist with specified, assigned tasks and/or missions.

6. Domains are interdependent and JFCs are responsible to integrate and synchronize actions in multiple domains for achieving the desired effect.

This is not an inclusive list, but it does address a consensus of several key characteristics to establish domain dominance. In comparison, these traditional domain traits map directly to the character and structure of cyberspace domain as defined in the NMS-CO. The following is a point by point contrast:

1. Cyberspace is bounded by the electromagnetic spectrum (EMS). It represents the physical battle space or medium that provides for the uninterrupted flow of information. Although it can’t be seen, the EMS has measurable physical boundaries and can be expressed in terms of energy, wavelength, or frequency. Signals associated with any military operation can be measured within the EMS and are generated by physical platforms.

2. The goal of a JFC is to establish or affect information superiority. In order to do this in the cyberspace domain, the JFC must conduct warfighting activities in the EMS in order to gain control and momentum. Cyberspace domain capabilities include storing, modifying, disseminating, and employing information and the ability to deploy, operate, maneuver, and sustain the communication systems that provide these information services. This is accomplished through the unimpeded use of the EMS, which achieves information superiority enabling successful operations in all domains.

3. Military maneuver and operations occur routinely in the cyberspace battle space. Cyberspace operations have both a defense and offense dimension. Offensive activities include both kinetic and non-kinetic actions to disrupt or deny the enemy an uninterrupted flow of information. This includes a kinetic strike on a critical C4 node, Electronic Warfare or Computer Network Attacks. Defensive examples include actions to maneuver C4 platforms to a secure location, implementing information assurance vulnerability assessment, COMSEC or upgrading computer system firewalls.

4. The Cyberspace domain employs specialized equipment that requires unique training to be effective. Communication systems and computer networks are needed to store, modify, and disseminate information. The training required is diverse and specialized, and varies from high end technical skills (satellite communications and satellite operators to computer analysts) to lower end technical skills (cable installers).

5. Unified Command Plan changes resulted in new DOD missions, organizational structure changes, and roles and responsibilities that are distinct and unique to cyberspace and the information battle space. The services have taken different approaches in cyber-type organizations and tasks, but each service has taken steps to

operate and dominate the domain. The importance of information superiority is a common understanding throughout the DOD and is reflected in doctrine and information strategies.

6. Successful operations in every warfighting domain require situational awareness and decision-making information. JFC's position themselves to acquire this capability through the control of EMS. Activities such as space control and network planning are integrated throughout the operational continuum to ensure this effect. Likewise, offensive operations in other domains support the cyberspace battle space (i.e., jamming, kinetic destruction of a telephone switching center) by denying the enemy the same capability.

The information environment and the cyberspace domain construct are complementary constructs. Together, they represent a complete information picture in warfighting. The cyberspace domain is the physical medium on par with air, land, sea, and space where warfighters leverage the battle space in support of a military operation. The EMS is that battlespace and has measurable physical boundaries that can be expressed in terms of energy, wavelength, and frequency. Signals and the platforms that produce them are confederated with the domain. It encompasses the physical platforms (servers, radios, and other systems and infrastructures) that generate the measurable elements of the medium. Communication and information systems platforms in the cyberspace domain bridge the information dimension to the information environment. The cyberspace domain enables the means to apply the information environment.

The Information Environment represents the character of information - content, relevancy and quality. Information superiority is measured in part by the relevancy, and accuracy of the command's information.[67] It has both the information and cognitive dimension qualities associated with it. The information environment is where battle space awareness exists and decisions are made that effect operations on the battle field. It enables the warfighter to create and act on information, which in turn ensures his capability to maintain situational awareness and decision superiority over an adversary. Through correlation and fusion of information, the information environment is the sole province of relevant information. The information environment and the cyberspace domain are interdependent. The ability to create and act on information works if there is a means to get it to the right people, at the right time in the right format.

The cyberspace domain enables military action in the other domains of land, sea, air and space. [68] It is critical to command and control, freedom of movement, decision-making and operational surety. As such it has distinct preeminent capabilities; without dominance in this domain, military operations in any domain can be muted, uncoordinated and ineffective.

Summary and Conclusions

Military application of new ideas and technologies often need something dramatic to break existing "old think" inertia. The most famous example of this is Billy Mitchell's use of airpower to sink the ex-German WWI battleship, Ostfriesland, at the time considered unsinkable. His efforts changed Naval doctrine and established a new (air) warfighting domain. Information warfare may represent the next true revolution in war fighting. Thus, it will require different insights into "weaponizing" information and force

application. These different insights can get its catalyst by DOD establishing a cyberspace domain in the same vein as it does the other domains; as a military operational environment in which combat is waged, information is the ordnance, and the communication and information systems are the weapon platforms.

The cyberspace domain and the information environment represent an information approach that invests JFCs to successfully conduct military operations in all domains. These changes will roadmap how the DOD actuates doctrine. New doctrine will drive tactics, processes and procedures to synchronize the employment of information and information enablers. In the process terminology, training, relationships, and responsibilities for U.S. forces become standardized. The results are habituated labors that allow the JFC to focus on solving the operational and tactical problems at hand.

This paper started by illustrating the divergence and confusion in information strategies and doctrine as a key reason for the passive, disjointed approach that undermines today's military's cyberspace operations. Then, a review of military command and control and history, and technology innovation featured the ironclad nexus between communication and information systems and military application. The enemy demonstrated intent and capability to attack U.S. vital interests with information operations and through the cyberspace domain to disrupt the flow of critical data and information. This followed with a review of the armed forces information related initiatives. On the positive side, the services recognize the importance of information and are diligent in developing doctrine to achieve information dominance. On the negative side, each service has interpreted existing strategies and doctrine differently, and taken different approaches that have dissipated the overall effort.

Next, we examined a potential solution. The premise of the solution is doctrinal acceptance of cyberspace as a physical domain comprised of electronics and communications networks that use electromagnetic energy. Equally noteworthy is the acceptance that it is discrete from the information that resides in it or flows through it. Finally, we tested the cyberspace domain construct to see if it was compatible in nature with the more traditional domains. This proved to be the case. All the warfighting functions in the cyberspace domain are aimed to affect a certain degree of dominance. A clear certitude is that to win the information war, the victor must gain and maintain information superiority through the domination of the cyberspace domain.

The doctrinal community must make a decision and demonstrate leadership to effect the required changes. The endstate is clear. A new domain is needed to effect information superiority. To stay the present course is an invitation to calamity. As Grace Hopper stated, “The most damaging phrase in the language is: "It's always been done that way."

Endnotes

[1] The Army’s mission is to fight and win our Nation’s wars by providing prompt, sustained land dominance across the full range of military operations and spectrum of conflict in support of combatant commanders. This is done by executing Title 10 and 32 United States Code directives, to include organizing, equipping and training forces for the conduct of prompt and sustained combat operations on land.

[2] Ibid.

[3] American Heritage Dictionary of the English Language (Boston: Houghton Mufflin Company, 2000), 533. U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, JP 1-02 (Washington D.C.: U.S. Joint Chiefs of Staff, amended through 14 September 2007). Domain is not defined in JP 1-02.

[4] U.S. Joint Chiefs of Staff, *Joint Operations,* JP 3-0 (Washington D.C.: U.S. Joint Chiefs of Staff, 10 Sep 2001). The four accepted domains are land, sea, air and space. This Joint Publication included a fifth domain termed information.

[5] U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Washington D.C.: U.S. Joint Chiefs of Staff, December 2006), 3. Hereafter stated as *National Military Strategy for Cyberspace Operations* (December 2006).

[6] U.S. Department of Defense Office of the Inspector General, *Joint Warfighting and Readiness: Management of Network Centric Warfare Within the Department of Defense*, D-2004-091 (Washington, D.C.: U.S. Department of the Defense, Office of the Inspector General, 22 June 2004). Hereafter stated as "Management of Network Centric Warfare Within the Department of Defense" (June 2004).

[7] This refers back to Elihu Roots quote at the beginning of the paper, "The real object of having an Army is to provide for war."

[8] Carl Von Clausewitz, *On War,* trans. Michael Howard and Peter Paret (New Jersey: Princeton University Press, 1976), 75.

[9] U.S. Joint Chiefs of Staff, *Joint Operations*, JP 3-0 (Washington D.C.: U.S. Joint Chiefs of Staff, 17 September 2006). Hereafter stated as *Joint Operations*, JP 3-0 (17 September 2006). Information Superiority is defined as the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

[10] Greg Rattray, *Strategic Warfare in Cyberspace* (London: MIT Press, 2001), 311.

[11] Ibid. The 1934 Communications Act gave the President the authority to take control of telecommunications assets during a national emergency. Other examples include: 1) The telegraph provided the means for President Lincoln to give strategic guidance to the Union's military operations from the White House to the battlefield. 2) During World War II, the radio was brilliantly exploited by the German army in prosecuting their "Blitzkrieg" tactics.

[12] Alan D. Campen, ed., *The First Information War: The Story of Communications, Computers and Intelligence Systems in the Persian Gulf War* (Fairfax, VA: AFCEA International Press, 1992), vi.

[13] Edward Waltz, *Information Warfare* (London: Artech House, 1998), 10.

[14] Campen, vii.

[15] Rattray, 315.

[16] U.S. Department of the Air Force, *Information Warfare* (Washington D.C.: U.S. Department of the Air Force, 1996).

[17] U.S. Department of the Army, *Information Operations*, FM 100-6 (Washington D.C.: U.S. Department of the Army, 27 August 1996) iv, v, 2-4.

[18] U.S. Joint Chiefs of Staff, *Joint Vision 2010* (Washington D.C.: U.S. Joint Chiefs of Staff, 1996), 16-19.

[19] U.S. Joint Chiefs of Staff, *Joint Vision 2020* (Washington DC: U.S. Joint Chiefs of Staff, June 2000); 28.

[20] U.S. Joint Chiefs of Staff, *Information Operations,* JP 3-13 (Washington D.C.: U.S. Joint Chiefs of Staff, 13 February 2006), GL-9. Hereafter stated as *Information Operations,* JP 3-13 (13 February 2006).

[21] Three current doctrines that discuss Information Operations and Information Superiority include: *Information Operations*, JP 3-13 (13 February 2006); U.S. Joint Chiefs of Staff, *Joint Communication Systems*, JP 6-0 (Washington D.C.: U.S. Joint Chiefs of Staff, 20 March 2006); and U.S. Department of the Army, *Operations: Tactics, Techniques, and Procedures,* FM 3-0 (Washington D.C.: U.S. Department of the Army, November 2003).

[22] *Information Operations,* JP 3-13 (13 February 2006). Information Operations also include Supporting and Related Capabilities. Supporting Capabilities include: Information Assurance, Physical Security, Physical Attack, Counterintelligence, and Combat Camera. Information Operations Related Capabilities: Public Affairs, Civil-Military Operations, and Diplomacy and Strategic Communications.

[23] *Joint Operations,* JP 3-0 (17 September 06), III-2.

[24] Ibid.

[25] U.S. Joint Chiefs of Staff, *Force Application Joint Functional Concept* (Washington D.C.: U.S. Joint Chiefs of Staff, 5 March 2004), Executive Summary. This Functional Concept is not approved at this time.

[26] Ibid.

[27] U.S. Joint Chiefs of Staff, *NetCentric Environment Joint Functional Concept* (Washington D.C.: U.S. Joint Chiefs of Staff, 7 April 2007). Hereafter stated as *NetCentric Environment Joint Functional Concept*, (7 April 2007).

[28] U.S. Joint Chiefs of Staff, *Joint Doctrine Development System,* CJCSI 5120.02 (Washington D.C.: U.S. Joint Chiefs of Staff, 30 November 2004).

[29] Sean P. Gorman, *Networks, Security and Complexity* (Northampton, MA: Edward Elgar Publishing, 2005), 23.

[30] Ibid.

[31] Ibid., 24.

[32] Qiao Liang and Wang Xiangsui, *Unrestricted Warfare* (Beijing: PLA Literature and Arts Publishing House, February 1999).

[33] Ibid., 47.

[34] Nathan Thornburg, “The Invasion of the Chinese Cyberspies,” *Time Magazine,* 29 August 2005; available from http://www.time.com/time/magazine/article; Internet; accessed 7 November 2007.

[35] Gorman, 24. Osama bin Laden issued this statement on 27 December 2001.

[36] Ibid., 22.

[37] Ibid.

[38] “Management of Network Centric Warfare Within the Department of Defense” (June 2004).

[39] *USSTRATCOM Home page*, available from www.stratcom.mil/fact_sheets/fact_jtf_ gno.html; Internet; accessed 11 January 2007. Joint Task Force Global Network Operations (JTF-GNO). JTF-GNO is located in Arlington, VA. JTF-GNO is USSTRATCOM’s operational component in directing the operation and defense of the Global Information Grid to assure timely and secure net-centric capabilities across strategic, operational and tactical boundaries in support of DOD’s full spectrum of warfighting, intelligence and business missions. JFCC-Network Warfare (JFCC-NW). The Commander, JFCC-NW) is dual hatted as Director, National Security Agency. This component facilitates cooperative engagement with other national entities in computer network defense and network warfare as part of the global information operations mission. This coordinated approach involves two other supporting commands. The Director, Defense Information Systems Agency also heads the Joint Task Force for Global Network Operations. This organization is responsible for operating and defending U.S. worldwide information networks, a function closely aligned with the efforts of the Joint Functional Component Command for Network Warfare. Joint Information Operations Warfare Command (JIOWC). The JIOWC plans, integrates, and synchronizes Information Operations (IO) in direct support of Joint Force Commanders and serves as the USSTRATCOM lead for enhancing IO across DOD. Located at Lackland AFB, Texas, the JIOWC deploys information operations planning teams worldwide at a moment's notice to support combatant commanders and joint task forces. Three objectives are outlined in the Joint Concept of Operations for GIG NetOps, Assured System and Network Availability, Assured Information Protection, and Assured Information Delivery must be achieved in order to secure information superiority.

[40] Josh Rogin, “Air Force Leaders Hold Cyber Summit,” *Federal Computer Week*, 9 February 2007; available from www.fcw.com/online/news/97618-1.html, Internet; accessed 10 November 2007.

[41] Ibid.

[42] *Information Operations,* JP 3-13 (13 February 2006), II-1 thru II-8. These core activities are psychological operations (PSYOP), military deception (MILDEC), and operations security (OPSEC). The employment of these and related activities; public affairs, civil-military operations and defense support to public diplomacy are need to apply the information element of combat power.

[43] Federal Computer Week Staff, “Army Considering Adding Cyberspace to Tactical Domains,” *Federal Computer Week*, 5 April 2007; available from

www.fcw.com/online/news/98157-1.html; Internet; accessed 16 December 2007. Comments made by the Honorable Vernon Bettencourt, Army Deputy Chief Information Officer.

[44] Ibid.

[45] U.S. Department of the Army, *Information Operations,* FM 3-13 (Washington, D.C.: U.S. Department of the Army, 28 November 2003), 7.

[46] U.S. Department of the Army, *Operations,* FM 3-0 (Washington, D.C.: U.S. Department of the Army, 27 February 2008), 7-2.

[47] Jim Hazuka and Maj Lee Cornelius, NORAD/USNORTHCOM J65 Staff Officers, email message to author, 5 October 2007.

[48] John C.K Daley, "US Air Force Prepares For Cyber Warfare," UPI International, 9 October 2006; available from www.spacewar.com/reports/US_Air_Force_Prepares_For_Cyber_Warfare_999.html; Internet; accessed 7 November 2007.

[49] Peter A. Buxbaum, "Air Force Explores the Next Frontier," *Government Computer News*, 2 February 2007; available from www.gcn.com/print/26_04/43153-1.html; Internet; accessed 5 January 2008.

[50] Henry Kenyon, "Cyberspace Command Logs In", *SIGNAL Magazine*, August 2007, 47.

[51] Ibid., 48. Comments made by Lt. Gen. Robert Elder the new organization's first chief.

[52] Ibid., 50.

[53] *Information Operations,* JP 3-13 (13 February 2006), II-4 thru II-5. The "hard power" core capabilities include Electronic Warfare (EW) and Computer Network Operations (CNO)- both attack and defend operations.

[54] David S. Alberts et al., *Understanding Information Age Warfare* (Washington D.C.: U.S. Department of Defense Command and Research Program, August 2001), 10-13. Hereafter stated as David S. Alberts et al., *Understanding Information Age Warfare.*

[55] *Information Operations,* JP 3-13 (13 February 2006), 1-1.

[56] Ibid.

[57] David S. Alberts et al., *Understanding Information Age Warfare*, 12-13.

[58] *Information Operations,* JP 3-13 (13 February 2006), 1-2.

[59] David S. Alberts et al., *Understanding Information Age Warfare*, 12.

[60] This is referenced in both *Information Operations,* JP 3-13 (13 February 2006), 1-2 and David S. Alberts et al., *Understanding Information Age Warfare,* 12.

[61] David S. Alberts et al., *Understanding Information Age Warfare*, 13.

[62] *Information Operations,* JP 3-13 (13 February 2006), 1-3.

[63] David S. Alberts et al., *Understanding Information Age Warfare*, 13-15.

[64] *National Military Strategy for Cyberspace Operations* (December 2006), 3.

[65] Ibid., 4.

[66] *Joint Operations*, JP 3-0 (17 September 2006), Chapters I, II, III, V and Appendix A.

[67] David S. Alberts, John J. Gartstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, (Washington D.C.: U.S. Department of the Defense Command and Research Program, February 2000), 32-33.

[68] *National Military Strategy for Cyberspace Operations* (December 2006), 4.