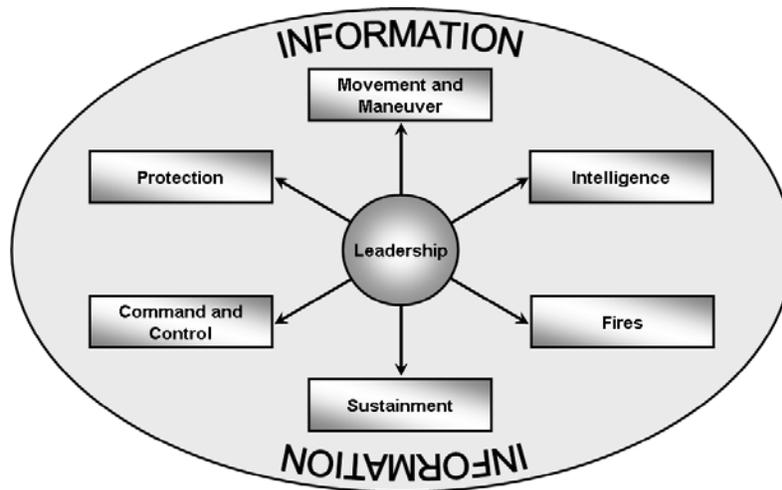


Information and Cyberspace Issue Paper #1: Information as an Element of Combat Power

INTRODUCTION

On 27 February 2008, the US Army unveiled its latest version of Field Manual (FM) 3-0, *Operations*. Among the significant changes in this capstone war fighting doctrine was the establishment of *information* as an element of combat power. “In modern conflict, information has become as important as lethal action in determining the outcome of operations. Commanders apply combat power through the war fighting functions using leadership and information.”



This paper begins the dialogue on the implications from this sea-change in the Army’s capstone operations doctrine. The resulting logic and precepts will be used to frame the revision of FM 3-13, which will be re-titled *Information*, thereby focusing on how the Army achieves the full potential of this pervasive element (both ways and means) to help secure national interests (ends) in an era of persistent conflict. Through this doctrinal process, the results of this dialogue also will result in concomitant changes across the other Army DOTMLPF domains: organizations, training, materiel, leadership and education, personnel, and facilities.

DISCUSSION

Although FM 3-0 designates *information* as an element of combat power and spends a few paragraphs as well as the entire Chapter 7 exploring this issue, the manual never defines *information*. Defining information as an element of combat power is a prerequisite to establishing the logical exposition on how commanders and staffs achieve its potential in full spectrum operations.

In the words of the *Stanford Encyclopedia of Philosophy*, *information* is a “notoriously” difficult concept to pin down, one that “can be associated with several explanations,” depending on the requirements of the person defining it.¹ In the view of one theorist, “information is...best conceived as a higher-order concept, rather than any specific thing.”² Joint Publication (JP) 1-02, *Department of Defense Dictionary of Military and Associated Terms* (12 Apr 01, as amended through 17 Oct 07), invokes JP 3-13.1, *Electronic Warfare*, as the source for its definition of *information* as, “1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.” However, JP 3-13.1 (25 Jan 07) does not include *information* in its glossary. Although these definitions for *information* are compatible with most common definitions in use today, neither they nor the others tell us much about *information as an element of, and elemental to, combat power* – the pervasive currency the force must leverage in full spectrum operations. (Nor, for that matter, are the definitions of much use to, say, a commander and his staff in Anbar Province, Iraq.)

¹ <http://plato.stanford.edu/entries/information-semantic/>; accessed March 4, 2008.

² Ibid.

Information and Cyberspace Issue Paper #1: Information as an Element of Combat Power

37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83

PROPOSED DEFINITION

Information is the element of combat power that empowers all other elements. It consists of meaningful facts, data, and impressions used to develop a common situational understanding; to enable battle command; and, to affect the operational environment.

SUPPORTING ARGUMENTS

Purists and pundits may argue data are the key -- that, in essence, information is data in context and, hence, the words “facts” and “impressions” are redundant. True, however the audience for this definition is not a group of information theorists but, rather, the Army writ large, the General Purpose Force which generally associates “data” with an esoteric concept used by those “outside the ropes.” The addition of “facts” and “impressions” to the definition serves to emphasize qualities of the higher-order in form more practical and common to the operational force.

Additionally, keeping in line with the aim of a *utilitarian* definition, the three-fold, use-specific aspects of the definition serve to capture broadly what it means to include information in the category of combat power. While more modest than an exhaustively technical definition, it makes clear information is both a necessary condition for, and a derivative effect of, the application of combat power. Hence, information is not merely an elemental aspect of combat power, but a potentially significant by-product of combat power, and a particularly valuable means to mold perception. Essentially, commanders and staffs use information in three ways.

- First, *information* serves as the means by which a unit develops knowledge about its operational environment. It is the substance gathered by all learning and collection processes, by which soldiers and leaders individually and collectively build and maintain situational understanding.
- Second, *information* forms the essential medium of the battle command process. It is the substance commanders use to understand the operational environment, to visualize, describe, direct and assess action, and to lead units to mission accomplishment.
- Finally, and in some ways most importantly for the purpose of this paper, and eventually FM 3-13, *information* – words, images, deeds, and digits – is the currency commanders use, both directly and indirectly, to achieve desired effects and to mitigate unintended consequences. Information in this context, as a derivative effect of operations, is particularly valuable as a means to lead critical populations toward decision making and behavior favorable to U.S. interests.

Finally, knowledge management professionals may not consider the proposed definition ideal for their purpose, but the definition does not violate their particular need, nor does it limit their utility.

IMPLICATIONS AND CONCLUSION

Defining information in this fashion provides an understandable and more applicable vocabulary for the bulk of the general purpose force. By establishing information’s inexorable linkage to the other elements of combat power and including the utilitarian uses of information for the operational force, this definition provides a useful framework for beginning to determine capability requirements and solutions across Army DOTMLPF necessary to leverage the power of information in an era of persistent conflict.

Information and Cyberspace Issue Paper #2: Integrating Information into the Battle Command Construct and the Operations Processes

INTRODUCTION

FM 3-0, *Operations* (February 2008), established *information* as an element of, and elemental to, combat power. Issue Paper #1 began examining the implications of this sea-change in the Army's capstone operations doctrine. The paper defined *Information* as "the element of combat power that empowers all other elements. It consists of meaningful facts, data, and impressions used to develop a common situational understanding; to enable battle command; and, to affect the operational environment."

This second issue paper considers how commanders and staffs can achieve the full potential of *information* by integrating it into the art of battle command and the operations process. The logic and precepts that result from the efforts that follow this series of issue papers will be used to revise FM 3-13, *Information*, and drive corresponding changes across the other Army DOTMLPF domains: organizations, training, materiel, leadership and education, personnel, and facilities.

DISCUSSION

The new FM 3-0 asserts the importance of achieving the potential power of information in full spectrum operations and invokes several imperatives for doing so, including the following two:

- Today's operational environment yields a high and often decisive impact to the side which best leverages information. As a result, commanders provide personal leadership, direction, and attention to it, fully integrating information into battle command.

- [Commanders] integrate information tasks into all operations and include them in the operations process from inception.

A recent survey of best practices in OPERATION ENDURING FREEDOM and OPERATION IRAQI FREEDOM included two important findings that pertain to this subject matter:

- First, commanders and leaders still struggle with the difficult task of integrating information into their battle command construct. Their education, training, and experience with the legacy paradigm of combined arms has ill-prepared them for the interactive complexity of 21st Century operations. Hence, this critical mission area is not part of their "DNA," notwithstanding their intuitive understanding of its importance.

- Second, the force continues to grope for a staff process that optimizes the power of information. There is no common practice for integrating informational activity with other operational activity within the operations process –

- 29% of respondents use the "Information Operations Working Group;"
- 29% use the "targeting process;"
- 27% use the "effects cell;"
- 5% use the operations process; and,
- 20% either invoked other methodologies or stated informational activity was not well integrated.

Supported by other analytical efforts – to include those by the Center for Army Lessons Learned; Strategic Studies Institute; Combat Studies Institute; symposia, conferences, and workshops; After-Action Reviews; interviews with commanders, and other studies – the best practices study urged a revision to the doctrine for integrating information into the operations process, followed by a comprehensive effort to ensure an orthodoxy for doing so was actualized in the force.

PROPOSED SOLUTION

Chapter 7, FM 3-0, delineates five tasks to leverage the power of information in full spectrum operations. The table below aligns staff responsibilities for synchronizing these tasks. This alignment has been a matter of considerable

Information and Cyberspace Issue Paper #2: Integrating Information into the Battle Command Construct and the Operations Processes

55 discussion and debate, beginning August 2006. The staff responsibilities were approved by CG, CAC, and CG,
 56 TRADOC, in January 2007 and by GEN Schoomaker and GEN Casey in their position as Army Chief of Staff in
 57 January 2007 and February 2008, respectively; however, the responsibilities were not included in the latest FM 3-0
 58 because it was decided this should be addressed at lower-level doctrine rather than in the Army's capstone
 59 operations doctrine.
 60

<i>Task</i>	<i>Information Engagement</i>	<i>Command and Control Warfare</i>	<i>Information Protection</i>	<i>Operations Security</i>	<i>Military Deception</i>
<i>Intended Effects</i>	<ul style="list-style-type: none"> • Inform and educate internal and external publics • Influence the behavior of target audiences 	<ul style="list-style-type: none"> • Degrade, disrupt, and destroy, and exploit enemy command and control 	<ul style="list-style-type: none"> • Protect friendly computer networks and communication means 	<ul style="list-style-type: none"> • Deny vital intelligence on friendly forces to hostile collection 	<ul style="list-style-type: none"> • Confuse enemy decision makers
<i>Capabilities</i>	<ul style="list-style-type: none"> • Leader and Soldier engagement • Public affairs • Psychological operations • Combat camera • Strategic Communication and Defense Support to Public Diplomacy 	<ul style="list-style-type: none"> • Physical attack • Electronic attack • Electronic warfare support • Computer network attack • Computer network exploitation 	<ul style="list-style-type: none"> • Information assurance • Computer network defense • Electronic protection 	<ul style="list-style-type: none"> • Operations security • Physical security • Counterintelligence 	<ul style="list-style-type: none"> • Military deception
<i>Staff Responsibility</i>	G-7 with PA, PSYOP and G-9 support within the information engagement cell	G-3 with G-2 support within the fires cell	G-6 within the Network Operations Cell	G-3; with G-2 support within the protection cell	G-5; within the plans cell

61 62 SUPPORTING ARGUMENTS

63
 64 The above construct aligns the capabilities associated with each of the information tasks with similar capabilities in
 65 the staff to ensure synchronization of like capabilities from inception. It emphasizes the use of doctrinal
 66 coordinating cells rather than ad-hoc groups as the way to integrate the appropriate activities into the operations
 67 process. The responsibility for achieving synergy, synchronization, and integration of all the organization's
 68 capabilities rests with the chief of staff. The chief of staff uses the G-3 to effect this synchronization in support of
 69 the commander's intent.

70
 71 The construct also places emphasis on the imperative to inform, educate, and/or influence perceptions, attitudes,
 72 beliefs, and behavior of relevant audiences in and beyond the commander's area of operations to facilitate mission
 73 accomplishment and promote enduring end states. Where once it was possible to treat "target audiences" as
 74 segregated entities to which one could send specific messages, however, today's interconnected community makes
 75 this highly improbable. This means messages may have wide-ranging and unpredicted effects, as they invariably
 76 reach unintended audiences. Fixing responsibility, authority, and accountability to the G-/S-7 not only leverages the
 77 power of *information*, but also harmonizes "messages" from the various staffs, ensuring desired effects are achieved.
 78

79 The construct is nested with the logic and tenets in the new FM 3-0, to include:

- 80
81 • *Information* is sometimes the decisive factor in campaigns and major operations. Effectively employed, it
82 multiplies the effects of friendly successes. Mishandled or ignored, it can lead to devastating reversals.

Information and Cyberspace Issue Paper #2: Integrating Information into the Battle Command Construct and the Operations Processes

83
84 • Full spectrum operations in the information age require a comprehensive approach to *information*. In
85 particular, Army operations emphasize the importance of peoples' perceptions, beliefs, and behavior to the success
86 or failure of full spectrum operations and in the persistent conflicts the Nation continues to face.

87
88 • *Information* is commanders' business. Commanders at every level require and use *information* to seize,
89 retain, and exploit the initiative and achieve decisive results. Therefore, commanders must understand it, integrating
90 it in full spectrum operations as carefully as fires, maneuver, protection, and sustainment.

91
92 • Soldiers' actions are the most powerful component of *information*. Visible actions coordinated with
93 carefully chosen, truthful words influence audiences more than either does alone. Consistency contributes to the
94 success of friendly operations. Conversely, if actions and messages are inconsistent and/or incongruent, friendly
95 forces lose credibility. Loss of credibility makes land forces vulnerable to enemy and adversary actions and places
96 the mission and Soldiers at risk.

97
98 • Battle command is the art and science of understanding, visualizing, describing, directing, leading, and
99 assessing forces to impose the commander's will on a hostile, thinking, and adaptive enemy. Battle command
100 applies leadership to translate decisions into actions—by synchronizing forces and warfighting functions in time,
101 space, and purpose—to accomplish missions.

102
103 • Commanders understand, visualize, describe, direct, lead, and assess throughout the operations process.
104 They: develop a personal and in-depth understanding of the enemy and operational environment; visualize the
105 desired end state and a broad concept of how to shape the current conditions into the end state; describe their
106 visualization through the commander's intent, planning guidance, and concept of operations in a way that brings
107 clarity to an uncertain situation, to include expressing gaps in relevant information as commander's critical
108 information requirements (CCIRs); direct actions to achieve results; and, continuously assess the situation and adapt
109 execution accordingly. Commanders anticipate and accept prudent risk if needed to create opportunities to seize,
110 retain, and exploit the initiative and achieve decisive results. Most of all, commanders lead by force of example and
111 personal presence, inspiring people to uncommon accomplishments.

112
113 • Commanders promote the leadership and initiative of subordinates through mission command. They accept
114 setbacks that stem from the initiative of subordinates. They understand land warfare is chaotic and unpredictable
115 and action is preferable to passivity. Thus, they encourage subordinates to accept calculated risks to create
116 opportunities, while providing intent and control that allow for latitude and discretion.

117 118 **IMPLICATIONS AND CONCLUSION**

119
120 Deciding what audiences – enemy, adversary, neutral, or friendly – are relevant to a particular mission and what
121 cognitive effects are required must become an integral aspect of battle command from the moment the mission is
122 received or perceived. Deciding what actions, words, and images, used where and in what sequence, to achieve
123 those effects is the essence of the concept of the operation. In effect, the ultimate goal must be to synchronize
124 operations to our messages. As such, *information* must be commanders' business.

125
126 The modular force must have a common bias toward action – an orthodoxy for planning, preparing, and executing
127 full spectrum operations. The criticality of information as an element of, and elemental to, combat power cannot be
128 relegated to a parallel or bifurcated process where one part of the organization orchestrates this part of the operation
129 while the Chief of Staff, G3, and G5 orchestrate the remainder. Such parallel processes result, at best, in de-
130 confliction rather than in true integration and optimum combat power that comes by the complementary arrangement
131 of information and other operational activity via the operations process and its supporting coordinating cells. If
132 information is commanders' business, then responsibility for its integration with other operational activity must rest
133 with the Chief of Staff, albeit he may delegate authority to the G-3.

Information and Cyberspace Issue Paper #3: Defining Cyberspace

INTRODUCTION

The first battles in cyberspace seem to have begun with the first major attacks in 1998 when anti-Chinese riots in Indonesia ignited retaliation from Chinese hackers.¹ Subsequent organized attacks followed the bombing of the Chinese Embassy in 1999, the EP-3 incident in 2001, and a series of organized attacks dubbed "Titan Rain" that targeted the U.S. military and defense industrial bases from 2003-2005.^{2,3} 2007 was the year previous attacks and battles in cyberspace were dwarfed by what has been coined Cyber War I or Web War I. On April 26, the Baltic country of Estonia became the target of a sophisticated and well-orchestrated campaign in cyberspace following political tensions with Russia. There were 1000 attacks on the first day and then 2000 attacks per hour on subsequent days. This continued for 23 days and the Estonian government and financial institutions were essentially shut down.⁴

Recognizing this unique and growing threat, the U.S. published its National Strategy to Secure Cyberspace in February 2003. The strategy recognized "...the way business is transacted, government operates, and national defense is conducted has changed...that these activities now rely on an interdependent network of information technology infrastructures called cyberspace."⁵ The National Military Strategy for Cyberspace Operations (NMS-CO), published in 2006, expanded the definition of *cyberspace* to "a domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networked systems and associated physical infrastructures." There has been considerable debate by the Joint Staff and amongst the Services over this "working" definition of cyberspace, but to date no consensus has been reached.

The U.S. Army must reach consensus on a definition soonest to proceed with the development of capabilities to operate in cyberspace. Hence, this paper is intended to promote the dialogue necessary to develop the Army's definition of cyberspace. The description will serve as the basis for follow-on efforts across the Army domains of doctrine, organizations, training, materiel, leadership and education, personnel, and facilities (DOTMLPF).

DISCUSSION

In addition to the above NMS-CO definition, the following four definitions merit consideration in our drive to develop the U.S. Army's definition of *cyberspace*:

- "Cyberspace means the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." (NSPD-54)

- "Cyberspace: a global domain within the information environment consisting of the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." (DoD, 21 Feb 2008)

- "Cyberspace as a 'domain' within the information environment that transcends the four physical domains, where networked electronic systems, the electromagnetic spectrum, and associated physical infrastructures are used to create, store, modify and exchange data." (Joint Forces Command (JFCOM) and Joint Staff J-7)

- "Cyberspace is the virtual battlefield created when one electronic system is used to communicate with and in some way change another." USMC White Paper on Cyberspace submitted for Chase Essay Contest.

¹ Scott J. Henderson, *Dark Visitor*, Lulu Press, 2007, p 6.

² Ibid.

³ Bradley Graham, Hackers Attack Via Chinese Web Sites: U.S. Agencies'; Networks Among Targets, August 25, 2005, <http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html>

⁴ Multiple sources including *Wall Street Journal*, *NY Times*, and *Washington Post* articles

⁵ National Strategy to Secure Cyberspace, February 2003

Information and Cyberspace Issue Paper #3: Defining Cyberspace

48 While each of these definitions has merit, none offers a sufficiently holistic view of the problem set to allow the
49 Army to frame the military problem as the Land Component for full spectrum operations. The NSPD-54 definition
50 is a collection of “things” and does not describe cyberspace as a component of the operational environment. This
51 definition may be more appropriate for a broader Homeland Security perspective, but inadequate for full spectrum
52 operations. The NMS-CO definitions do not state how cyberspace relates to the four physical domains: air, sea,
53 space, and land. This is critical to the Army because of the cross-domain coordination that will be required for
54 successful operations in cyberspace. The JFCOM/J-7 definition diminishes the importance of cyberspace by
55 subjugating cyberspace to the information environment, yet still transcending the other domains. *Cyberspace* and
56 *Information* are complementary but separate entities with significant overlap within the operational environment,
57 rather than subordinating either to the other. The DoD definition modifies the NSPD-54 definition by stating that
58 Cyberspace is a global domain but then subjugates it to the information environment again. The Marine Corps paper
59 seeks to bind cyberspace within a militarily relevant definition; however, it does not recognize cyberspace
60 transcends military interests, or that DoD is tasked by the NMS-CO to secure cyberspace to protect the defense
61 industrial base. Indeed, DoD, joint forces, and services are conducting daily operations at the enterprise level.⁶ Of
62 all the definitions, the Marine Corps’ is a good start toward developing the definition of cyberspace best suited for
63 full spectrum operations and the starting point for a concept of operations.

64

65 PROPOSED DEFINITION

66

67 *Cyberspace* is the domain that transcends the four physical domains and is characterized by the use of electronics
68 and the electromagnetic spectrum to create, store, modify, and exchange data via networks across the operational
69 environment.^{7 8}

70

71 SUPPORTING ARGUMENTS

72

73 Current operations show the vital importance of electronic warfare and computer network operations capabilities but
74 a series of cyber battles over the past ten years give new insight on cyberspace. Cyberspace is truly a unique, real
75 battlefield that must be addressed in a holistic manner. Cyberspace is a contested part of the operational
76 environment. The military problem is to determine how to ensure friendly access to - and freedom of action in -
77 cyberspace, and at the same time to deny the adversary the same. Cyberspace, and the broader electromagnetic
78 spectrum (EMS), are optimized by leaders and Soldiers who understand both the technical and operational
79 dimensions of this realm of the operational environment, and who are outfitted with cyber and electronic capabilities
80 that enable a broad range of operational activity, to include empowering information while concurrently reducing
81 risk to the force.

82

83 Specifically, the definition comprises seven key components:

84

⁶ The enterprise level is important to the Army because it is a critical vulnerability. Information stolen in attacks at the enterprise level directly affects knowledge about capabilities and vulnerabilities. For example, the Army’s helicopter mission planning system was stolen during the “Titan Rain” attacks. Sensitive but unclassified information can also be used in asymmetric attacks. Imagine if an adversary stole military pay, unit rosters, DTS records, and pre-deployment/training briefs. A clever adversary could change a soldier’s pay status, conduct a mass identity theft attack on a deploying or deployed unit, initiate phantom rape or infidelity charges on key unit personnel based on information on travel claims and in pre-deployment/training briefs, and many other attacks. These attacks would impact a unit’s ability to train; a soldier’s ability to focus on the mission; cause hardships on military families; and require huge amounts of time and effort to investigate and resolve the situations.

⁷ This definition deletes “networked systems and associated physical infrastructure” from the NMS-CO and JFCOM/J-7 definitions because they are parts of networks. The danger in taking these out of the definition is that they highlight key areas that need to be defended and also takes the emphasis off the physical aspects of cyberspace. The network hardware, the physical use of the EMS and the associated physical infrastructure are all key aspects of what distinguishes information from cyberspace.

⁸ Cyber is also not defined in Joint or Army doctrine. The CNO-EW Proponent proposes the following definition: **Cyber**: relating to computer and electronic networks.

Information and Cyberspace Issue Paper #3: Defining Cyberspace

85 1) **Relationship to the four physical domains.** Cyberspace, unlike the land, air, space, and sea domains, is
86 man-made and uses a portion of the EMS as a medium to share and exchange data. Cyberspace transcends and is
87 the vital integrator of the other four physical domains. The danger here is to ignore the physical properties of the
88 cyberspace domain. Data is physically created, stored, and modified by electronic systems, transferred via physical
89 infrastructures such as fiber optic cables or through the EMS.

90
91 2) **Electronics.** Electronics are the hardware components with associated software applications that allow the
92 creation, storage, modification, and exchange of data to create information.

93
94 3) **The electromagnetic spectrum (EMS).** Cyberspace uses portions of the electromagnetic spectrum to
95 store, modify, and exchange data. Cyberspace is man made and uses only a portion of the naturally occurring EMS.

96
97 4) **The ability to create, store, modify, and exchange data.** Electronics create and store, and modify data to
98 create information. Electronics use networks as a means to exchange and an alternative means to store and modify
99 data and information. Just because computers or other electronic devices can be networked used to create, store,
100 modify and/or exchange data does not mean they are in operating in cyberspace – they must be networked.

101
102 5) **Networks.** Connectivity between electronics creates a network. The US military relies on networks and
103 networked systems for conducting operations and for the asymmetric advantage of a shorter OODA Loop than our
104 adversaries. In fact, the Army's Modular Force will create a system of systems as a center of gravity. Networked
105 systems and associated physical infrastructures could be shortened to just networks in the definition but that would
106 reduce the importance of the associated physical infrastructures.

107
108 6) **The operational environment.** Cyberspace is a contested part of the operational environment and must be
109 included in any Intelligence Preparation of the Environment. What makes cyberspace unique is that there is a global
110 enterprise level in addition to the normal strategic, operational, and tactical levels.

111
112 7) **Domain.** DoD and C,JCS have labeled cyberspace as a domain, which recognizes the significant
113 challenges associated with operations in cyberspace. The importance of the challenges, the enormity of the
114 challenges, the complexity of the challenges, the duration and cost of the challenges, and the legal, ethical, political,
115 and diplomatic sensitivities associated with the challenges all reinforce the decision to define cyberspace as a
116 domain. Defining cyberspace as a domain also enables the Army to take a holistic approach in its analysis and to
117 overlay a framework that can be used to facilitate the complex coordination and integration required across the joint,
118 interagency, intergovernmental, and multinational community of practice. Cyberspace is also a domain because it is
119 a place where all six of the joint functions are executed.⁹

120
121 *Cyberspace* characteristics significantly differ from the air, land, sea and space domains. To conduct operations in
122 cyberspace, the Army must understand and describe the characteristics of this domain.¹⁰

123
124 1) **Cyberspace transcends the other four physical domains of Air, Land, Maritime, and Space.**
125 Cyberspace is physically integrated through nodes and links that physically reside in the Air, Land, Maritime, and
126 Space domains.

127
128 2) **Cyberspace is a non-contiguous domain.** Cyberspace is becoming increasingly interconnected, but
129 networks within cyberspace can be, and often are, isolated or closed. Protocols, firewalls, encryption, and physical
130 separation from other networks are all means of isolating networks from each other. Many computer networks are
131 isolated from the each other simply because there is no connection that is the result of the initial design, the network
132 technologies, the type of network, or the network purpose. For example, a hard-wired network without any radio-
133 frequency (RF) connectivity is isolated from most RF intrusion.

⁹ Joint Publication 3-0, Joint Operations, establishes the six Joint functions as Command and Control, intelligence, fires, movement and maneuver, sustainment, and protection.

¹⁰ Much of this section was based ideas presented in Air Force Doctrine Document 2-X bottom line draft 3.1, February 04, 2008 and multiple other conversations.

Information and Cyberspace Issue Paper #3: Defining Cyberspace

135 3) **Cyberspace is a diverse domain.** Cyberspace is actually a collection of smaller segments or systems of
136 systems. It is made up of many different types of networks with many different functions, levels of
137 interconnectivity, technical complexity, vulnerabilities, and other characteristics.
138

139 4) **Cyberspace is continually changing and evolving.** The cyberspace domain is expanding and evolving as
140 communications technology and the market expand and evolve. In other words, the segments within cyberspace
141 continuously change due to technical innovation; the addition, removal, replacement, or reconfiguration of
142 components; and updated protocols. Cyberspace is also temporal; since it is man-made, users can disconnect from it
143 (unless another user has planted Trojan Horses or other means to keep the user connected.)
144

145 5) **Operations in cyberspace can occur at nearly the speed of light.** Since electrons travel at the speed of
146 light, many actions in cyberspace are nearly instantaneous. The United States can attack, or be attacked, with a
147 speed not achievable in the other domains. Depending on the degree of interconnectivity, this can happen over
148 global distances. Therefore, defensive measures must account for rapid decision-cycle requirements to respond to
149 attack and offensive measures must be flexible enough to account for fleeting targets.
150

151 6) **Similar to the other domains, operations in cyberspace include maneuver.** This can be seen when an
152 adversary moves from one component or node in the friendly network to another until a vulnerability is discovered.
153 Code writing has also been called maneuver where software engineers write code to move around protection
154 mechanisms in a network.
155

156 7) **Cyberspace Contains Logical and Physical Maneuver Space.** Cyberspace segments are connected by
157 physical infrastructure and electronic systems that use the EMS. This is the physical maneuver space within the
158 EMS where different parts of the physical network are probed looking for vulnerabilities and ways around protective
159 measures. Code writing is a form of logical maneuver because it allows an unauthorized user to try to gain and
160 maintain access to a system by exploiting a fault in defensive logic. One of the most dangerous parts of logical
161 maneuver is if an unauthorized user is not identified, the user may be able to create authorized access to the system
162 for future attacks.¹¹
163

164 **IMPLICATIONS AND CONCLUSION**

165

166 Operations in cyberspace are critical for the Army and the Land Component. The U.S. Army must reach consensus
167 on a cyberspace definition soonest to proceed with the development of future capabilities to operate in cyberspace.
168 These capabilities will be required to enable the vision of the future modular force and associated Future Combat
169 Systems in supporting full spectrum operations and joint interdependency requirements. The proposed definition is
170 conducive to full spectrum operations within the larger context of promoting national security objectives.
171

172 The proposed definition enables the Army to integrate and maximize capabilities by describing cyberspace as:

- 174 1) A medium through which information is shared, transmitted, and manipulated.
- 175
- 176 2) The combined sum of physical, virtual and ethereal networks that enable commanders to manipulate and
177 share data and information in order to create effects throughout the operational environment.
178
- 179 3) That portion of the electromagnetic spectrum that enables information exchange among electronic
180 components in the four physical domains (Land, Air, Sea, and Space).

¹¹ This future attack may degrade or disrupt the system at the worst possible time during friendly operations or actions.

Information and Cyberspace Issue Paper #4: The Relationship Between Information & Cyberspace

INTRODUCTION

Issue Papers #1 and #3 established proposed definitions for both *information* as an element of, and elemental to, combat power and *cyberspace* as a domain through which information and other activities pass – a domain that is increasingly contested. The purpose of this issue paper is to delineate clearly the relationship between the two. It is particularly important to establish this relationship because the word “information” is often used or understood to gain unique significance when associated with technology. The reality, of course, is that the Army wants to leverage all the technological advantages it can in the five domains: land, sea, space, air, and cyberspace. Operations in and through cyberspace provide unique opportunities to create cognitive and physical effects and shape the operational environment. Nevertheless, capitalizing on the power of information remains vital to mission success even when the nearest computer network is miles away.

PROPOSED THESIS

In the context of full spectrum operations, *Information* is the currency of understanding, decision-making, and action while *cyberspace* is a domain in the operational environment in and through which cognitive and physical effects can be created.

DISCUSSION

Issue Paper #1 addressed *information* as an element of, and elemental to, combat power and defined it as, “The element of combat power that empowers all the other elements. It consists of meaningful facts, data, and impressions used to develop a common situation understanding; to enable battle command, and to affect the operational environment.” As true in the 1860s for GEN Ulysses S. Grant as it is today for GEN David Petraeus, the operative word in the definition is “meaningful.” As an element of combat power, *information* relies on its relationship to human will and decision-making. The “facts, data, and impressions” to which humans assign meaning flow through all the multi-variant aspects of the physical universe, all the “domains” available. Some have argued the application of physical pain is a most “meaningful” way for transmitting information to a human – a notion not too disparate from the assertion in FM 3-0 that action is the clearest and most effective form of communication.

Issue Paper #3 defined cyberspace as, “The domain that transcends the four physical domains and is characterized by the use of electronics and the electromagnetic spectrum to create, store, modify, and exchange data via networks across the operational environment.” Another way to think about cyberspace is to consider it a man-made domain that uses the electromagnetic spectrum and is contiguous to and increasingly pervasive throughout the other domains of land, air, sea, and space. As is the case with the four physical domains, cyberspace forms a dimension of the operational environment which may be contested or not as the exigencies of a given conflict and interests of the protagonists dictate. As with the other domains, cyberspace can become the venue for its own unique form of operational activity (hacker wars, for example), and it also can serve as a medium through which combat power can be projected to affect specific aspects of other domains.

IMPLICATIONS AND CONCLUSION

Adopting the proposed construct – “In the context of full spectrum operations, *Information* is the currency of understanding, decision-making, and action while *cyberspace* is a domain in the operational environment in and through which cognitive and physical effects can be created.” -- clarifies the relationship between information and cyberspace. Cyberspace can be the venue for its own “wars,” and it can comprise a very important medium through which information is handled, but not the only medium. Similarly, information is but one activity that uses cyberspace. Keeping this distinction in mind will help avoid category errors, distinguishing properly between ends, ways, and means in the application of combat power to the Nation’s

Information and Cyberspace Issue Paper #4: The Relationship Between Information & Cyberspace

55 business. This construct also will help avoid mistaking the task of building Army capability and capacity
56 for conducting operations in and through cyberspace with that of developing Army capability and capacity
57 for capitalizing on the power of information in full-spectrum operations.