ARMY INFORMATION CENTERS OF GRAVITY: CAN WE PROTECT THEM?

A MONOGRAPH
BY
Major Rosemary M. Carter
Signal Corps

MENS EST CLAVIS VICTORIAE

School of Advanced Military Studies
United States Army Command and General Staff College
Fort Leavenworth, Kansas

Second Term AY 98-99

19991109 053

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
		MONOGRAPH

4. TITLE AND SUBTITLE

Army Information Centers of Gravity: Can We Protect Them?

5. FUNDING NUMBERS

6. AUTHOR(S)

MAJOR Rosemary Carter

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

School of Advanced Military Studies
Command and General Staff College
Fort Leavenworth, Kansas 66027

8. PERFORMING ORGANIZATION REPORT NUMBER

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

Command and General Staff College
Fort Leavenworth, Kansas 66027

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE;
DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

included in monograph

14. SUBJECT TERMS

Information Operations ; Information Centers of Gravity; Information Warfare

15. NUMBER OF PAGES
57

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED
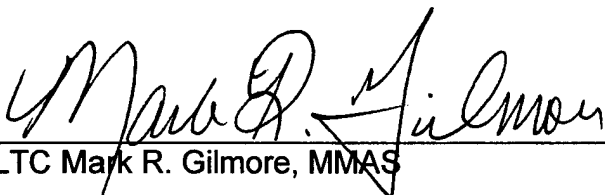
SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Rosemary M. Carter

Title of Monograph: *Army Information Centers of Gravity: Can We Protect Them?*

Approved by:

_____ Monograph Director
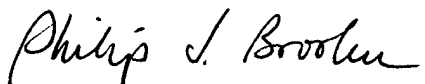LTC Mark R. Gilmore, MMAS

_____ Director, School of Advanced
LTC Robin P. Swan, MMAS   Military Studies

_____ Director, Graduate Degree
Philip J. Brookes, Ph.D.   Program

Accepted this 27th Day of May 1999

ABSTRACT

ARMY INFORMATION CENTERS OF GRAVITY: CAN WE PROTECT THEM? by MAJ Rosemary M. Carter, USA, 46 pages.

As the Army keeps pace with the information age, it must determine how to leverage information to win its wars. According to Brigadier General Wayne M. Hall information is a tool for influencing an enemy's decision cycles. This is achieved by attacking the enemy's information centers of gravity. BG Hall defines these information centers of gravity as the "physical place or mental construct in cyberspace where a confluence of intellect, decisions, collection, automation, communications and planning occurs."

The purpose of this monograph is to determine if the US Army has information centers of gravity and if so, can they be protected. The monograph first determined the key components of information from the definition of information superiority. These key components were analyzed using three criteria to determine the Army's information centers of gravity. The criteria used were their influence on decision cycles, effects on strategic aims, and impact on combat power. The analysis concluded that there are two information centers of gravity - Army commanders and information operations cells.

The monograph used the Army's defensive IO capabilities to determine if it can protect these information centers of gravity. The conclusion is that the US Army does have the capability to provide protection for these information centers of gravity. The monograph concluded with a look at additional initiatives that are ongoing to protect both information centers of gravity and the key components of information that support these centers.

TABLE OF CONTENTS

Introduction

Background

Information Operations (IO) is one of the buzzwords for the strategic thinkers in our Army. It has become an integral part of every model for current and future operations. Joint Publication 3.0, Joint Doctrine for Information Operations, defines IO as "actions taken to effect adversary information and information systems while defending one's own information and information systems."[1] This definition is supported by the Army's IO Integrating Concept Team's Draft of FM 100-6, Information Operations: Tactics, Techniques and Procedures, dated June 1998, which defines IO as "that degree of dominance in the information domain, which permits the conduct of operations without effective opposition. Army operations address it as a window of opportunity created by focused effort that allows the actions or beliefs of the enemy commander to be influenced in support of decisive operations."[2] This draft of FM 100-6 defines IO as a subcomponent of Information Superiority. IO is divided into two components - offensive IO and defensive IO. These and other related terms are further defined in chapter two of this monograph.

In describing IO warfare in his recent paper, *Reflections on 21st Century Information Operations*, Brigadier General Wayne M. Hall, Military Intelligence Corps background, stated that "IO will be primarily a war of wits - it's a struggle for initiative, relative advantage, and mental agility. .... in IO, the primary struggle will be for control of or influence on an opponent's decision making. One of the ways to achieve this influence is to attack the opponent's INFORMATION CENTERS OF GRAVITY."[3] He

defines the information centers of gravity as the "physical place or mental construct in cyberspace where a confluence of intellect, decisions, collection, automation, communications and planning occurs."[4] BG Hall does not identify the US Army's information centers of gravity.

This monograph attempts to identify these information centers of gravity for the United States Army. This discussion is significant because the Army must identify the components of information operations that are the source of its information dominance in order to develop systems to protect them.

Protect is defined in FM 100-5-1, Operational Terms and Graphics, as "a tactical task to prevent observation of or engagement or interference with, a force or location; all actions taken to guard against espionage or capture of sensitive equipment and information."[5] This definition complements the Random House Dictionary definition: "to defend or guard from attack, invasion, loss, annoyance, insult etc.; cover or shield from injury or danger."[6] This monograph modifies the doctrinal definition to accommodate the strategic level as follows: all actions taken to prevent observation of or engagement or interference with, a force or location; all actions taken to guard against espionage or capture of sensitive information.

Defining the Research Question

The overarching question is - Can the US Army protect those information operations and systems that are absolutely necessary for it to accomplish its missions?

Method of Analysis and Structure

This monograph answers the overall question by establishing clear definitions for the terms and concepts involved and using these definitions to answer three supporting questions. Chapter two defines the terms. First, it defines information operations and all of its components. The sources for these terms is the newly published Joint Publication 3-13, Joint Doctrine for Information Operations, dated 9 October 1998, and the Army's current draft of FM 100-6, Information Operations: Tactics, Techniques and Procedures, dated June 1998. Use of the draft FM 100-6 instead of the current version is outlined in chapter two. This chapter also defines information centers of gravity. Because it is not a doctrinal term, BG Hall's paper is the source for the definition. However, the monograph also researches the discrepancy between centers of gravity defined by Clausewitz as the "hub of all power"[7] and current doctrinal definitions as well as BG Hall's stipulation that information is not a source of power but a means of power.

Chapter two also answers the first supporting question - What are the Army's current defensive IO capabilities? These are based on current systems and doctrine. These capabilities were used during the analysis of the Army's ability to protect its information centers of gravity.

Chapter three answers the second supporting question - What are the Army's information centers of gravity? To answer this question, the monograph identifies the key components for each category and subcategory of information superiority (relevant information (RI), information systems (INFOSYS) and information operations (IO)). Components can be tangible systems and equipment or intangibles based on synergy developed with IO. These key components were assessed as centers of gravity based on

3

three criteria: influence on the Army's decision cycles; effects on the Army's strategic aims; and impact on combat power.

Chapter four answers the third supporting question - What is the Army's ability to protect these information centers of gravity? The analysis uses the current capabilities within the components of defensive IO that are defined in chapter two. The analysis is quantitative, based on the existence of capability, and qualitative, based on this author's assessment of the feasibility of that capability. Answering this third supporting question results in the answer to the overarching research question.

Conclusion and Recommendations

The monograph bases its conclusions on the answers to the three supporting research questions. The answer to the first question is the definitions of the Army's current defensive capabilities. These capabilities are: physical security, OPSEC, counterdeception, counter-PSYOP, counterintelligence, and electronic protect (EP). Public affairs and civil affairs support these capabilities. Chapter three answers the second research question by determining that the Army commanders and information operations cells (IO cells) are the information centers of gravity. The final research question is answered in chapter four in which it is determined that the Army can protect these two information centers of gravity with the defensive IO capabilities. The monograph makes several recommendations in the final chapter to expand beyond the delimiters of this paper. These delimiters are defined below.

4

Delimiters

The primary delimiter of this monograph is its prescribed length. The length limitation effects the entire scope of the monograph. First, this delimiter narrows the study of Army defensive IO capabilities to those currently in place within the Army. Projections of future organizations and capabilities are certainly important but are not considered here. Additionally, the length limits the type of information operations to defensive. While offensive IO is an effective tool for deterrence, it will not be addressed.

The length limitation also limits the monograph's analysis of information centers of gravity. A thorough analysis should determine these centers of gravity uniquely for each of the types of military actions - offense, defense, stability and support operations. Army information centers of gravity may be adjusted based on the type of action and the elements of METT-T. However, this monograph is limited to the overarching information centers of gravity that generically apply across all four types of actions.

This monograph also limits the threats to our Army's information centers of gravity to threats from foreign countries. The length limitation does not allow for consideration of other threats to include hackers, industrial espionage, insiders, other authorized users, or criminals and organized crime. All of these are viable and very real threats that must be considered but are outside of the scope of this monograph. The final delimiter is the classification of the monograph. Because the monograph is unclassified, it does not consider special information operations.

Defining Terms

This chapter provides the background and definitions for the monograph. The first section defines terminology for discussing information and its functions. The second section provides a definition for information centers of gravity based on BG Wayne Hall's thesis and historical definitions of center of gravity. Finally, this chapter identifies the Army's current defensive IO capabilities.

Information Terminology

The arena of information and its functions is constantly evolving. Part of this evolution is resolving the numerous terms used to define the environment. In current doctrine, the Army definitions are not nested within the joint doctrine. Additionally, the terms as defined in the IO Integrating Concept Team Draft, dated June 1998 of FM 100-6, Information Operations: Tactics, Techniques and Procedures, are different from definitions in the current FM 100-6, Information Operations, dated 6 December 1995.

To minimize confusion throughout this monograph, the primary sources of defining terminology are Joint Publication 3-13, Joint Doctrine for Information Operations (JP 3-13) and the Army's June 98 draft of FM 100-6. Army terminology is used because this monograph focuses on Army issues. Joint definitions are used if an Army definition does not exist or to further explain a term or concept. In the cases where the Army definition differs from the joint definition, the Army definition is used because the focus of the monograph is an Army issue. The monograph does not have the length allowance to conduct a comparison of the Army and Joint definitions and terminology.

The most recent draft of FM 100-6 is used instead of the current FM 100-6 because the terminology in the draft is aligned with the terms in the joint publication. The 1996 version of FM 100-6, which is the current manual, used terms no longer recognized in the joint community. Although the revised manual is still in draft, the new terminology is being taught by the Battle Command Training Program (BCTP)[8] and in the Command and General Staff College's Information Operations course.[9]

The highest level of information control is information superiority (IS). IS is "that degree of dominance in the information domain which permits the conduct of operations without effective opposition. Army operations address it as a window of opportunity created by focused effort that allows the actions or beliefs of the enemy commander to be influenced in support of decisive operations."[10] IS is comprised of three interrelated components: relevant information (RI), information systems (INFOSYS), and information operations (IO). RI is defined as "all relevant information of importance to the commander in the exercise of command and control; includes information about friendly forces, the enemy, potential adversaries, neutrals and operations are to facilitate decision making."[11] Information systems (INFOSYS) is defined as "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display and disseminate information."[12] Information operations (IO) is defined as "offensive and defensive actions at each echelon in peace and war to defeat the adversary's command, control, computers, communications, intelligence, surveillance, and reconnaissance (C4ISR); effect adversary and influence neutral leaders; and protect friendly information and information systems plus the command and control process. The major IO capabilities are operational security (OPSEC), psychological

7

operations (PSYOP), military deception, electronic warfare (EW), physical destruction, and computer network attack (CNA). Related IO activities include public affairs, civil affairs, and other interactions with news agencies."[13] This Army definition for IO is compatible with the joint definition which is "actions taken to effect adversary information and information systems while defending one's own information and information systems."[14]

IO is categorized as either offensive IO or defensive IO. Offensive IO is defined in both joint doctrine and FM 100-6(D) as "the integrated use of assigned and supporting capabilities and activities mutually supported by intelligence, to effect adversary decision makers to achieve or promote specific objectives."[15] The IO capabilities that support offensive IO include OPSEC, military deception, PSYOP, electronic warfare, physical destruction, special IO,[16] support from civil affairs and public affairs, and computer network attack. Defensive IO is "the integration and coordination of policies and procedures, operations, personnel, and technology to protect information and defend information systems.[17] Defensive IO is further discussed at the end of this chapter.

Defining Centers of Gravity

The definition of information centers of gravity begins with a definition of center of gravity. The term 'center of gravity' was introduced by Carl von Clausewitz in his book on the military theory titled On War. Clausewitz based his writing on the campaigns of Napoleon Bonaparte in the late 18th/early 19th centuries. Because the book was published by Clausewitz's wife from his notes, the work is not a finished document. However, of the eight books within the work, books one, two and eight are

generally considered the most complete.[18] The relative completeness of the individual

books is important because of some of the inconsistencies within Clausewitz's own

definitions of and use of the term. His definition from book eight, one of the most

complete sections, states that the center of gravity is "the hub of all power and

movement, on which everything depends."[19] The concept of center(s) of gravity has

evolved from Clausewitz - being defined, adapted and sometimes bastardized by military

theorists and historians.

An example of the modifications to Clausewitz's term is Air Force Colonel John

Warden's definition for his systems analysis of an enemy. In his article "The Enemy As

a System," published in the Spring 1995 edition of the *Airpower Journal,* COL Warden

defined centers of gravity as "rings of vulnerability, ... absolutely critical to the

functioning of a state."[20] COL Warden identifies specific centers of gravity at both the

strategic and operational levels.[21] While his theory is compelling and his five-ring model

was arguably an effective tool during the planning of the air campaign in Operation

Desert Storm, the interpretation of 'center of gravity' as always being an enemy

vulnerability is a huge leap from Clausewitz's theory that centers of gravity are strengths.

These discrepancies between definitions are still evident in our doctrine today.

Chart A-1 located in Appendix A depicts the joint and service definitions for centers of

gravity. The first obvious discrepancy between definitions is the use of singularity and

plurality. The joint definition allows for multiple centers of gravity but they must relate

to a military force. The Army definition specifies one center of gravity but does not limit

it to military specific items. The Navy copies the joint definition with the exception of

limiting it to one center and highlighting the fact that it applies to both friendly and

enemy forces. The Air Force has adopted the joint definition, while the Marine Corps focuses on enemy vulnerabilities rather than centers of gravity.

The debate on singularity or plurality of centers of gravity is beyond the scope of this monograph. For purposes of this monograph the plural definition is used. The selection of plurality is validated by Carl von Clausewitz's statements that the military planner should always search for the one omnipotent hub of the enemy's power. However, where that was not possible, he recommended decisive attacks on one hub with the anticipated result of effecting the other centers of gravity. When this did not work, Clausewitz recommended attacks on multiple centers of gravity.[22]

The debate as to whether a center of gravity must always be a military force is beyond the scope of this monograph. However, because this monograph addresses IO, which in its capabilities and effects is often outside the standard definitions of military forces and capabilities, the definition of center of gravity used in this monograph is the broader definition. For the purposes of this monograph the term 'centers of gravity' is defined as "those characteristics, capabilities, or localities from which an entity derives its freedom of action, physical strength or will to fight."

Information Centers of Gravity

In his paper, <u>Reflections on 21st Century Information Operations</u>, Brigadier General Wayne Hall proposes the concept of information centers of gravity. He defines them as the "physical place or mental construct in cyberspace where a confluence of intellect, decisions, collection, automation, communications, and planning occurs. An information center of gravity is of such importance that manipulation or control of this

center of power and energy will go far in enabling either side to achieve their aims or conversely jeopardize mission accomplishment."[23]

Can information truly be a center of gravity? The first consideration for this debate is information's position as one of the four instruments of national power. Joint Publication 1, Warfare in the US Armed Forces, (JP-1) includes 'information' as one of the instruments of national power along with diplomacy, the military and economics. Referred to with the acronym DIME, the four instruments are used as a framework for the National Security Council to assist the President in development of the National Security Strategy. This grand strategy is supported by the Chairman, Joint Chiefs of Staff, with the National Military Strategy.[24] The National Military Strategy uses the DIME to balance the military source of power with the other three sources. Since information is a source of power at the strategic level then it meets the definition of a possible center of gravity.

However, in his paper, BG Hall states that "information isn't power like the old adage claims. ... information is the means to power and that it takes the art of battle command to turn information into actual, usable power. Understanding of this phrase - *INFORMATION IS THE MEANS TO POWER* - is the heart of successful IO. (emphasis original)"[25] Can a 'means' be a center of gravity? In his article "Information, Technology, and the Center of Gravity" published in the *Navy War College Review*, LCDR Jeffrey A. Harley considers the impact of information on the center of gravity concept. LCDR Harley expresses concern that the technical successes of the Gulf War will result in an unfounded reliance on technology as the decisive advantage in the next conflict. He says that "the proliferation of information technologies has led to the

11

impression that information is itself a center of gravity, which has in turn confused both the role of information and the center of gravity concept. Information seems to have been transformed from a means to an end."[26] The author argues that exploitation of information is not new. While he readily admits that technology has drastically increased the complexity and vulnerabilities of information flow, he says that "victory is achieved not by defeating his information but by beating his armed forces."[27]

Alternately, the work of COL John Boyd, USAF, appears to support the 'means' as a center of gravity. COL Boyd was the first theorist to combine aspects of logic theories with the laws of thermodynamics when he completed his "Destruction and Creation" study on the relationships between competition and conflict. His theory asserted that rather than attacking actual, physical centers of gravity, "one should create *noncooperative centers of gravity* by attacking the moral-mental-physical linkages which bind the hubs together."[28] In Boyd's theory, the goal is paralysis of the enemy by disrupting his ability to make decisions. This is done by confusing the enemy commander's perceptions of reality through deception and misinformation. Once the commander can no longer discriminate between fiction and reality, he can no longer make effective decisions. His 'means' of making decisions has been damaged or destroyed.

But should COL Boyd's term *noncooperative centers of gravity* be considered a validation of 'means' as centers of gravity as it is currently defined? An alternative view is that these links are more closely defined as decisive points. Joint Pub 3.0 states that when a direct attack is not feasible or preferable, the commander should consider an indirect approach. The manual then discussed decisive points stating that "decisive

points are not centers of gravity; they are the keys to attacking protected centers of gravity."[29] The publication describes these decisive points as usually geographical but states that they may include other items such as critical boundaries or airspace. This definition, if broadened to cover the aspects of information superiority, is a more appropriate description of Boyd's linkages. Therefore, when information is used as a 'means' it is a decisive point. This does not discredit the previous conclusion that information, when it is a source of power, meets the definition of information center of gravity. However, the role of information must be carefully scrutinized to discriminate between true information centers of gravity and information components that are decisive points for other centers of gravity.

Defensive IO Capabilities

Defensive IO "integrates and coordinates policies and procedures, operations, personnel and technology to protect and defend information and information systems."[30] Defensive IO is conducted through information assurance (IA), physical security, OPSEC, counter-deception, counter-PSYOP, counter intelligence (CI), electronic protection (EP), and special information operations (SIO)[31]. Defense IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."[32] The following are detailed definitions and descriptions of the Army's defensive IO capabilities:

Information Assurance (IA). IA is the process of detecting, restoring, responding, and deterring enemy information.[33] Information Assurance is an endstate

that is achieved by successfully implementing the other defensive IO capabilities resulting in a reduction in the vulnerabilities to our information superiority.

Physical Security. According to Joint Pub 1-02, <u>DoD Dictionary of Military and Associated Terms</u>, physical security is "that part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents and to safeguard them against espionage, sabotage, damage and theft."[34] Physical security as part of IO is the physical measures taken to safeguard all elements of IS - relevant information, information systems, and information operations. In wartime the Army's physical security capability is its fighting force. This force is comprised of every soldier and system that has the potential to defend against an aggressor. It includes the maneuver units, fire support systems, and military police as well as communications specialists and cooks given the mission to defend a position. It is an integral part of every operation executed by the Army. In the garrison environment, the Army also has its fighting force to execute physical security operations. In many cases, they do. However, the peace-time Army often defers this mission to contracted security forces or automated systems. This does not negate the potential to use military force.

OPSEC. OPSEC is defined in FM 101-5-1, <u>Operational Terms and Graphics</u>, as "all measures taken to maintain security and achieve tactical surprise." It includes countersurveillance, physical security, signal security, and information security. It also involves the identification and elimination or control of indicators, which can be exploited by hostile intelligence organizations. It is the protection of friendly information against enemy collection and exploitation. OPSEC is an integral aspect of any military

operation but is critical during military deception operations. OPSEC is often considered an aspect of either military intelligence operations or communications systems operations, but it is the responsibility of all Army personnel. OPSEC is a consideration in military planning.

Counterdeception. Military Deception is defined in JCS Publication 1-02 as "those measures designed to mislead the enemy by manipulation, distortion or falsification of evidence to induce him to react in a manner prejudicial to his interests."[35] It further defines five categories: strategic military deception, operational military deception, tactical military deception, service military deception, and military deception that support OPSEC. Counterdeception are plans and operations designed to negate the effects of an adversary's deception.[36] Counterdeception includes both broad procedures to counter the adversary's ability to plan a deception and specific operations designed to counter an identified deception operation. Counterdeception, like deception operations, is executed by any elements of the military force. Counterdeception does not include the intelligence responsibility of identifying enemy deception operations.

Counter-PSYOP. According to Joint Publication 1-02, and FM 33-1, Psychological Operations, PSYOP are operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups and individuals. The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. These threats are defined in FM 33-1 as "any person, institution, or environmental factor that presents an identifiable, recurring obstacle to the: success of a PSYOP program; execution of the commander's mission; or

achievement of national policy objectives. ... A thoroughly developed and well-implemented PSYOP program can exploit any factor and fulfill PSYOP goals."[37] This type of program is counter-PSYOP. Counter-PSYOP is planned and executed using the same doctrine, techniques and procedures as other forms of psychological operations. Part of the PSYOP planning process is the identification of threats to PSYOP.

The Department of the Army's Deputy Chief of Staff for Operations and Plans (DCSOPS) is responsible for coordinating formulation of PSYOP policy to guide operational employment of PSYOP personnel.[38] Because the majority of the United States psychological operations are executed in the joint environment,[39] the Army's PSYOP policies must be in line with joint doctrine. At the joint level, US Special Operations Command (USSOCOM) is the unified combatant command for special operations, to include PSYOP. The Secretary of Defense assigns all CONUS-based PSYOP forces to the USCINCSOC. CINCSOC is not assigned a geographic area of responsibility for normal operations. He normally acts as a supporting CINC for one of the regional CINCs, although he may be designated the commander of special operations forces within a joint command structure.[40]

The army's PSYOP assets are assigned to the US Army Civil Affairs and PSYOP Command (USACAPOC), a major subordinate command of the US Army Special Operations Command (USASOC). The Army assets include both active duty forces and reserve component forces. The active component PSYOP Group, located at Ft Bragg, NC, plans and conducts PSYOP activities worldwide. It develops, coordinates and executes PSYOP in peacetime and assists the CINC in executing these functions in time of war.[41] The reserve component Tactical Support Group (TSG) provides tactical

PSYOP support for forward deployed US forces.

Counterintelligence (CI). As defined in FM 101-5-1, Operational Terms and Graphics, CI is "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities."[42] According to FM 34-1, Intelligence and Electronic Warfare Operations, the "essence of the Army CI mission is to support force protection. ... CI is a multi-discipline function designed to defeat or degrade threat intelligence targeting capabilities. MDCI (multi-discipline CI) operations support force protection through support to OPSEC, deception, and rear area operations across the range of military operations. .... MDCI personnel advise deception planners on the vulnerabilities of threat foreign intelligence services (FISs) and associated battlefield collection systems to various friendly deception capabilities and techniques."[43] CI is an element of force protection that may encompass several of the other defensive IO capabilities. CI support can include PSYOP, deception/counter deception, OPSEC, and physical security.

Electronic Protect (EP). EP is a component of electronic warfare. Electronic warfare is defined in FM 34-10, Division Intelligence and Electronic Warfare Operations, as "the use of electromagnetic or directed energy to degrade, neutralize, or destroy enemy combat capability."[44] It includes jamming and electromagnetic deception. EW consists of three areas: electronic attack (EA), electronic warfare support (ES) and electronic protection (EP)[45]. As stated above, EP is considered defensive EW. "EP protects personnel, facilities, or equipment from the effects of friendly or enemy EW which

17

degrades or destroys friendly communications and non-communications capabilities.
Good electromagnetic emanation practices are the key to a successful defense against the
enemy's attempt to destroy or disrupt our communications and non-communications
systems."[46] The goal of EP is to eliminate patterns in electromagnetic emanations,
making it difficult for the enemy to target our systems.

Two other activities that support IO are public affairs and civil affairs. Although
they are not components of defensive IO they are discussed in the monograph and so are
defined here. Public affairs (PA) is defined in JP 1-02 and FM 46-1, Public Affairs
Operations, as those "public information and community relations activities directed
toward the general public by the various elements of the Department of Defense. PA is
necessary at the strategic, operational, and tactical levels of war to influence soldier
morale, unit cohesion, (and) public opinion; effect strategic goals; impact operational
objectives and have a bearing on tactical execution."[47] The Army's requirement to
conduct PA is derived from Title 10, US Code which appoints the Secretary of the Army
as the responsible agent for public affairs operations. PA operations must achieve a
careful balance between OPSEC and flow of timely information. When used properly
and with the necessary command involvement, PA is an effective tool to maximize US
public support, fight rumors and enemy disinformation operations, and undermine
efficient operations. It helps the commander to achieve information dominance.[48]

According to FM 101-5-1 and FM 41-10, Civil Affairs Operations, civil affairs
(CA) are matters concerning the relationship between military forces deployed into a
country or area and the civil authorities and people of that country or area. The CA
mission is to support the commander's relationship with civil authorities and civilian

populace, promote mission legitimacy and enhance military effectiveness.[49] This mission has two parts - conducting civil-military operations and providing support for the civil administration. While the first part is support to the Army commander and the second part is support to stabilize a foreign government, they are totally interdependent missions that must be synchronized and coordinated to represent unity of effort. When operating in the support to civil administration role, CA meets the United State's obligations derived from our international treaties, agreements and law. When used as part of the overall plan, CA supports political, economic and informational goals as well as military objectives.[50]

Army Information Centers of Gravity

The purpose of this chapter is to identify the Army's information centers of gravity. They are derived from the key components for each of the three areas of information superiority (RI, INFOSYS and IO). These components are analyzed against three criteria to determine the centers of gravity. The criteria are: influence on the Army's decision cycles, effects on the Army's strategic aims, and impact on combat power. The components must meet all three criteria to be an Information Center of Gravity. The criteria are further defined in the next paragraphs.

Defining Criteria

Influence on the Army's decision cycles is defined using Boyd's theory of the OODA loop. Boyd's theory views any conflict as a battle where each leader must observe (O) his enemy, orient (O) himself and his forces to best challenge the enemy, decide (D) on the most appropriate action, and act (A).[51] The hypothesis is describes as a loop because it is a continuing cycle with feedback at every level. COL Boyd argued that any military's tactics, strategy, and technologies should all be based on executing our OODA loops faster than the enemy - getting inside of his decision cycle by executing ours faster. Using the stages of Boyd's OODA loop - observe, orient, decide and act - as the basis for the criteria, the analysis determines if the identified key components are necessary for the US Army's OODA loop to maintain its current speed.

The second criterion is effects on the Army's strategic aims. As defined in the Department of the Army's document United States Army Posture Statement FY00, the

Army's strategic aims are the same as those outlined in the Department of Defense's National Military Strategy. They are: shaping the international environment, response to crises, and preparation for tomorrow's challenges. The Army has capabilities to support each of these aims. The Army supports its shaping strategy through peacetime engagement programs, forward deployed forces, peace operations, and combined exercises. According to the posture statement, "the Army's unique and robust shaping capabilities give it the lead role in the first pillar (shaping) of the NMS."[52] To support the second strategic aim of rapid response, the Army maintains trained and ready units available for deployment on short notice. The Army also maintains forward-positioned forces and prepositioned assets to minimize response times. To meet the aim of being prepared for the future, the Army is "implementing a comprehensive transformation strategy to build the information-age capabilities needed to protect our interests well into the 21st century while preserving current readiness levels."[53] This monograph analyzes the key components to determine if they are necessary to achieve the Army's strategic aims of shaping, responding and preparing.

The third criterion is impact on combat power. The Army's manual FM 100-5, Operations, defines combat power as the synergistic effects of maneuver, fire power, protection and leadership. According the field manual "overwhelming combat power is the ability to focus sufficient force to ensure success and deny the enemy any chance of escape or effective retaliation. The enemy is killed, wounded, captured, or not capable of influencing future battlefield events; he is frozen by fear and uncertainty, confused, and isolated. Overwhelming combat power is achieved when all combat elements are violently brought to bear quickly, giving the enemy no opportunity to respond with

coordinated or effective opposition."[54] The smallest Army unit that is self-sustaining is the division. The division contains the organic resources to plan and execute independent operations to leverage combat power against an enemy. Under the total Army concept there are ten active duty divisions and eight National Guard divisions. According to FM 71-100, <u>Division Operations</u>, "the success of Army operations depends on the success of its divisions."[55] Army divisions have traditionally fought as part of an Army corps. However, they are also capable with some staff augmentation of deploying as an Army forces (ARFOR) headquarters under a Joint Task Force. For the purposes of this monograph "impact on combat power" is defined as impact on the Army's division's capabilities. Capabilities includes warfighting and force projection of CONUS-based divisions. According to FM 100-5, leadership is the most essential element of combat power. Leadership is addressed as one of the key components of information superiority and therefore is not included here as part of the criteria.

Identifying Key Components

In order to identify the key components of information superiority that are considered as information centers of gravity, each area of IS is considered. First a look at relevant information (RI). RI is divided into three areas: information about friendly forces, information about other players (enemy/adversarial/neutral forces) and information about the operations area. Information about friendly forces is maintained at all levels of the Army. Units operating from a table of organization and equipment (TOE) from company through corps maintain their personnel, training and equipment status of readiness via the unit status report (USR). Unit status reports are filed monthly

by active duty units and quarterly by reserve component forces. The USR is used to determine the overall readiness of the Army's combat force. The data contained in the Army's USR is classified, but it is also time sensitive and easily replaceable. The data changes with each reporting period and can be regenerated by the system.

In addition to the USR, the Army maintains readiness information on non-tactical (non-TOE) organizations via their commander's reports to their MACOM. For example, the fixed-station communications community uses system outage reports and monthly status of communications reports to inform Signal Command of its readiness based on its mission of providing tactical and strategic communications to the elements of the warfighting Unified Commands and operating the Army portion of the Defense Communications System (DCS).[56] Another example is the installation status report that "provides assessments of installation readiness to perform missions such as supporting deployments and conducting mobilization training."[57] While many of these reports are classified, as with the USR, they are simply a status of an Army system. Additionally, the data for these reports is easily regenerated by the system because it is only a representation of a system in the Army.

Information about other players is the second portion of RI. In the past, the focus on information about the other players was on information about the "enemy." However, in recent years this category has expanded, along with the expansion of the Army's mission, to include peace operations. It now can include forces friendly to the United States but belligerent towards each other, non-governmental agencies operating in a given area, and other third parties. In all cases, the information is collected primarily by United States intelligence agencies. The intelligence community is composed of the Army's

resources, the resources of the other services, and national intelligence agencies such as the National Security Agency (NSA) and the Central Intelligence Agency (CIA). In accordance with FM 34-1, the "mission of Army intelligence is to provide timely, relevant, accurate and synchronized IEW support to tactical, operational, and strategic commanders across the range of military operations."[58] Intelligence is echeloned into strategic, operational and tactical intelligence levels, however, the echelonment is for visualizing the flow of intelligence, allocation of resources and assignment of tasks. Echelonment is not linked to the sources of intelligence for the commander on the ground. Commanders at all levels are provided intelligence from each level of intelligence.[59] The information collected and analyzed by the intelligence community is not stored in a central date base. It is collected and stored with agencies throughout the community. Intelligence requirements or requests for intelligence information (RFIs) are processed through the intelligence chain of command. In many cases, an RFI generates responses from multiple sources. What is key to this monograph is that there is not one identifiable entity that can be called the Army's intelligence information source. Intelligence is provided by a myriad of systems that are by their nature redundant.

The final area of RI is information about a given area of operations. This type of information includes geographical data, weather data, and demographics. While the internet and other research means can provide volumes of data about a given area, the intelligence community is still responsible for analysis of this data to provide commander's with usable intelligence. This intelligence information is collected and stored by the intelligence community in the same types of data bases that are used to store other intelligence information.

Information systems is the second area to consider. According to FM 100-6 (D), INFOSYS include "personnel, machines, manual or automated procedures, and systems that allow the collection, processing, dissemination, and display of information."[60] INFOSYS are the personnel, hardware and organizations that process information within the Army.

The first portion of INFOSYS is the Army personnel that handle information. They include every soldier, government civilian and contractor that collects, stores, processes and make decisions based on information. In broad terms this category can include everyone involved with the Army. For purposes of this monograph these soldiers, government civilians and contractors that install, operate and maintain (IOM) information systems are considered to be components of that system. Therefore, a discussion of the Department of Defense's Global Command and Control System inherently includes all the personnel that IOM the system to include the soldier operating the terminal in the TOC, the system administrator managing the system, and the contractor maintaining the telecommunications link.

Separate and unique from the system operators are the Army commanders. These commanders must exercise both leadership and decision making.[61] FM 100-5 defines leadership as "taking responsibility for decisions; being loyal to subordinates; inspiring and directing assigned forces and resources toward a purposeful end; establishing a teamwork climate that engenders success; demonstrating moral and physical courage in the face of adversity; providing the vision that both focuses and anticipates the future courses of action."[62] In accordance with Joint Pub 3-13, Joint Doctrine for Information Operations, commanders are responsible to integrate IO into the deliberate and crisis

planning processes to incorporate its disciplines and capabilities into all actions.[63] The

qualities of leadership are especially critical for information superiority because the goal

is to quickly and lethally effect the physical, moral, and cybernetic domains of the

enemy. The commander is at the top of the hierarchy that executes this goal and is

therefore a key component of IS. For purposes of this monograph, the commander is not

only the individual that it currently filling that position, but includes our entire leadership

development process that produces US Army leaders. It includes the philosophies,

training programs, command climate and experiences that result in the unique leadership

qualities of these commanders. Therefore, 'commander' does not refer to a specific

individual but to a process, and all the individuals that are a product of that process and

currently or potentially fill the positions.

The hardware and infrastructure portion of INFOSYS includes our data networks,

voice systems and data storage facilities. The goal for these systems is to provide a

seamless architecture from the strategic to the tactical levels to facilitate success in joint

and combined operations. The systems are designed to be robust through vertical and

horizontal integration. The primary warfighting data INFOSYS is the Global Command

and Control System (GCCS).[64] It is a joint system that interfaces with the Army GCCS

(AGCCS). AGCCS supports garrison operations for submission of the monthly unit

status report and other recurring reports. It is also the operational level commander's

warfighting command and control system. It is a deployable system serving as the

operational level interface for the Army Battle Command System network. This network

is comprised of fixed, semi-permanent and mobile networks to include the AGCCS,

Army Tactical Command and Control System (ATCCS) and the Battle Command

Brigade and Below System (FBSB2) currently being fielded. The ATCCS interfaces directly into the AGCCS providing a seamless link from the tactical operating center into the Army's infrastructure. It is made up of five components; the maneuver control system, the advanced field artillery tactical data system, the forward air defense C2 and intelligence system, and the combat service and support system.

In addition to these command and control systems, and according to a 1998 Government Accounting Office report, the Army currently has thirty seven independent networks,[65] as well as its segment of Department of Defense networks. Although the Army is currently executing the Army Enterprise Architecture (AEA) to develop and maintain an integrated information system that is in compliance with joint standards,[66] many of these networks are currently on unique platforms with proprietary software. Primarily, these are the data networks that support the sustainment base for the Army and comprise the Standard Army Management Information Systems (STAMIS) - logistical, medical and personnel information management systems. These systems provide information flow from the tactical level back to the sustaining base. They are used for both garrison operations and deployed forces. An example is the Army's unit logistics support system (ULSS) that is used for managing the unit supply systems.

The Department of Defense is currently implementing the Defense Information Systems Network (DISN) as "the common-user, long-haul telecommunications network for all Defense components."[67] The purpose of the network is to reduce costs by establishing larger contracts. While DISN is an effective cost savings measure for the Department of Defense, its consolidation of networks increases the risk of large scale outages due to equipment failures, contractor issues or attacks on the system. While the

transition plan for moving the Army's independent networks to this system is not complete, using previous Defense Information Systems Agency (DISA) transition plans as a model, the systems will transition as existing contracts expire. Some networks will receive permanent waivers, however, the final DISA criteria for granting permanent waivers is not complete so it is impossible to determine what the final number of independent systems will be.

Complementary to the Army's data networks are its voice services that include the Army-owned local switchboards, local US telephone companies, FTS2000 contract,[68] the Defense Switched Network (DSN), and host nation telephone systems. These unclassified voice systems are encrypted as required using end-to-end encryption devices such as the STU-III telephone terminal. The voice circuits are increasingly used for data transmission of electronic mail and other point-to-point data transfers. While none of these systems were designed for data transmissions, the increased capabilities of modem devices and improvements to the commercial telecommunications systems make these data transfers both feasible and effective.

The Army's tactical communications systems, Mobile Subscriber Equipment (MSE) and triservice tactical (TRITAC) systems provide the hardware and network protocols for establishing both networking and voice services for deployed forces. The systems may be closed networks only allowing processing of voice calls and data transfers within the tactical system. However, more commonly they are connected to the strategic voice and data networks (both military closed and commercial systems) via gateways. Access to the wider networks may be limited using software controls, but the hardwire connection exists between the systems. These connections make the systems

vulnerable to outside computer network attacks.

In addition to this tactical network, communications systems have been supplemented during recent longer term deployments, such as the deployment to Haiti and current operations in Bosnia, with commercially contracted networks. Contracted services for deployed forces are technically similar to the fixed-communications contracts found in our garrison Army. The primary difference is the duration and flexibility of the networks. The systems are unclassified using off-the-shelf technology to provide a semi-permanent communications architecture.

These numerous types of networks are categorized for this monograph into three types of networks. They are: strategic C2 networks, other strategic networks and tactical networks. Strategic C2 networks are clearly defined. The other strategic networks include the components of the STAMIS networks, the voice networks used for data transfers, and the Army systems processed over DISN systems. The tactical networks include both the Army communications equipment and the commercial contracts supporting deployed tactical units.

Another area of INFOSYS is data storage facilities. These include both manual storage facilities and the Army's electronic databases. Most of the Army's long term paper storage is transferred to microfilm or microfiche to reduce the space requirements. More recently these files are being transferred to electronic storage to eliminate space requirements and reduce the cost of maintaining the documents. Storage repositories exist for the finance system (now a Department of Defense facility), the personnel permanent records storage, and the operational records. In addition the Army maintains historical records and files at several locations to include the Military History Institute at

Carlisle Barracks, PA, the Combat Studies Institute and Combined Arms Research

Library (CARL) at Ft Leavenworth, KS, the US Military Academy at West Point, NY,

and the major commands throughout the Army.[69]

Information operations is the last area of superiority. As defined in chapter one of

this monograph, information operations are actions taken to effect adversary's

information and information systems while protecting one's own information and

information systems. IO consists of numerous capabilities that are defined within the two

major subdivisions of offensive and defensive IO. Offensive IO is actions that effect the

enemy's decision cycle. Defensive IO are actions that protect our decision cycles. The

capabilities that comprise offensive and defensive IO are: operational security (OPSEC),

electronic warfare (EW), physical attack/destruction, psychological operations (PSYOP),

deception/ counterdeception, counterintelligence (CI) and computer network attack

(CNA). Public affairs (PA) and civil affairs (CA) also contribute to IO although they are

not categorized as IO capabilities.[70] As discussed in chapter one of this monograph,

OPSEC, physical attack and deception are capabilities performed throughout the Army.

OPSEC is the responsibility of everyone. Physical attack directed against information

targets may be executed by any combat force in the Army, and deception may be

executed by any element in the Army. The other capabilities, although always a

commander's responsibility, are the missions of specific organizations. The capabilities

and responsible organizations are provided in Appendix A in table A-2. In this context,

organization is defined as military units, staff sections, or individuals that perform these

branch functions. These organizations are the executive agents for planning and

executing their IO capabilities, although they may be augmented by other forces or

capabilities. An example is counterdeception. While a Corps G2 counterdeception cell may plan an electronic signature to replicate the movement of forces to reinforce an enemy deception plan, the corps signal brigade may provide the communications systems to portray the signature. The G2 is still overall responsible for the mission.

While each of these organizations is responsible for some component of IO they are not responsible for IO in its entirety. IO may be a small part of their mission. An example of this is the intelligence staff. In other cases, such as the PSYOP forces, their entire mission is a capability of IO, but they handle only a small portion of the overall IO mission. According to new and emerging doctrine as well as current practices, the IO cell has overall responsibility for the planning, execution and management of information operations. The draft FM 100-6 creates information operations staff sections for both the corps and division levels. The mission for these sections is to plan, coordinate, direct, control, and monitor IO actions so that they become a combat multiplier for the commander.[71] Joint publication, JP 3-13, establishes a Joint Information Operations Cell to assist the J3 in exercising joint IO responsibilities.[72] Although neither manual specifically addresses the establishment of an Army component level IO cell, the joint publication directs the designation of "an IO point of contact or IO officer."[73] It is realistic to infer that an IO cell is established within the component G3 to serve as the IO staff. The Department of the Army has established the Land Information Warfare Activity (LIWA) to execute the IO functions at the service component level. Therefore, the Army and Joint staff are developing the doctrine for IO staffs for each level from Department of the Army down to division level.

During current operations in Bosnia-Hercegovina, an IO cell was established almost immediately to handle the unique nature of the operation. Numerous articles have captured the successes and lessons learned from this endeavor into IO. One of the early articles in the March/April 1997 *Military Review*, titled "Information Operations for the Ground Commander" captured the structure of the IO cell which included (and still does include today) LIWA field support teams. These IO staff sections provide the central location for the commander's IO planning. They are considered as key components of IO for further analysis as centers of gravity.

Based on the above discussions, the Army has numerous informational key components. Within the RI area they are adversary intelligence and friendly/operational intelligence. Within the INFOSYS area they are: Army commanders, strategic command and control networks, other strategic networks, tactical networks, and data storage facilities, and within the IO area they are the IO cells. These components are listed in Appendix A in table A-3 to provide easy reference. The remainder of this chapter analyzes these key components to determine if they are information centers of gravity.

Analysis

These key components are analyzed to determine if they meet the three criteria for information centers of gravity. The criteria, as defined in chapter two are: influence on decision cycles, effect on Army strategic aims, and impact on combat power. The first key component is adversary intelligence. Information about adversaries is critical for commanders to make decisions. The more detailed the analysis and conclusions based on that intelligence, the fewer assumptions the commander must make. This speeds both the

observation and orientation steps of Boyd's OODA Loop thus speeding up the decision. Lack of adversary intelligence increases the time required for these steps and slows the process.

Effect on the Army's strategic aims is the second criterion. The Army's strategic aims of shaping, responding and preparing are executed based on our ability to understand the world situation. However, adversary intelligence cannot drive the Army's strategic aims. These aims are developed based on the National Security Strategy and National Military Strategy. Adversary intelligence influences how the Army executes these aims, not how they are developed, and therefore does not meet the second criterion. The final criterion is the impact on combat power. This criterion addresses the 'how' of implementing the strategic aims. Adversary intelligence is used by the division commander to leverage the principals of war of mass and economy of force. Developing and reviewing intelligence is the first step in planning any division operations. Adversary intelligence meets the third criterion of impacting on combat power which validates it as a key component of information superiority. However, because it does not meet all three criterion, it is not an information center of gravity.

The second key component is friendly/operational intelligence. An analysis of this component follows the same logic as the analysis for adversary intelligence. Friendly/operational intelligence impacts on the Army's decision cycles because is speeds the observation and orientation steps of the OODA loop. It is a combat multiplier for the division commander. However, it is not a tool for developing the Army's strategic aims, but a tool necessary to implement those aims. Friendly/operational intelligence is a key component, but is not an information center of gravity.

Army commanders are the third key component. They are critical to Boyd's OODA loop. Their training, experiences and personal traits are the keystone of each step of the loop because they are making the decisions at each step. Without a doubt, they influence our decision cycles. Similarly, because the Army commanders are responsible for the development of the Army's strategic aims, they have an effect on those aims. Although the Army aims must be nested within the National Security Strategy, the experiences and personality of the leadership are evident in these aims. The third criterion is impact on combat power. As stated earlier in this monograph, leadership is the "most essential dynamic of combat power."[74] It therefore has the most effect on it. The capabilities of the divisions are directly effected by the training, teamwork and initiative of the soldiers within the division. These traits are directly impacted by the leadership of the division. This impact is felt at all levels from the command climate developed by the division commander down to the team-building capabilities of each squad leader. Army commanders have a thorough and lasting impact on combat power and are now defined as one of the Army's information centers of gravity.

Strategic C2 networks is the next key component. These networks are used by the Army to process and disseminate all types of information that is used to make decisions. All forms of intelligence requests are received and answered on these systems. Friendly and operational information is also passed. The systems are used to provide guidance, directives and orders throughout the Army. These systems therefore directly influence the speed of our decision cycles. The effect of these strategic C2 networks on a division's combat power is based on the size and type of missions of the division. If a division is wearing a JTF or Army Forces (ARFOR) hat, these networks are critical. If the division

is fighting as part of a major theater campaign, the networks are echelons above the division headquarters. However, the division will receive second or third order of effects of the networks, through national level traffic that is processed to them via tactical communications. The final criterion is effect on the strategic aims. These systems provide the primary communications conduit for the Army leadership. This tool is used in the development and maintenance of the Army's strategic aims. However, while timeliness is critical for decision cycles, it is not essential to the development of the Army's strategic aims. Therefore, while these strategic networks are an excellent tool for developing/maintaining these aims, they are not necessary. Strategic C2 networks remain a key component of IS, but are not an information center of gravity.

Do other strategic networks meet these criteria? The analysis for C2 networks applies to these networks also. The influence of these STAMIS networks on decision cycles and combat power vary based on the type of networks. However, none of them have a direct impact on the Army's strategic aims. They are not information centers of gravity. Tactical networks meet the first and third criteria. As part of the overall communications architecture, they process the information key to commanders making decisions on the battlefield. The success of these networks equates to real-time processing of information to commanders at all levels. This effects the speed of the decision cycles. Additionally, division-level tactical communications directly effect the capabilities of that division. Without a successful and reliable digital communications network, the division cannot quickly process calls-for-fire, nor plan a robust fire support plan incorporating all of its indirect fire capabilities. The AFATADS system facilitates massing of fires. The other tactical networks provide the same advanced capabilities to

their battlefield operating systems. However, these tactical networks do not effect the Army's strategic aims. By name and by function they are used at the tactical level of war. Therefore, while they are a critical key component of Army information superiority, they are not an information center of gravity.

The next key component is the US Army's data storage facilities. As with the intelligence components analyzed above, these facilities provide a service that is necessary for commanders to have the required tools for making fast and accurate decisions. These facilities have an impact on the observe and decide steps of the commander's decision cycle. These facilities are also used by the Army's highest leadership to develop and refine the Army's strategic aims. However, as with the intelligence components, these facilities do not effect our division's combat power and therefore do not meet the third criterion for an information center of gravity, though they remain key components of IS.

IO cells are the final key components. As defined above, these cells are defined in existing and emerging doctrine at all levels from brigade through Department of the Army. The Department of the Army's IO cell, the Land Information Warfare Office (LIWA), executes the both the offensive and defensive IO tasks at the service component level. With the mission to "provide the Department of the Army level information warfare/command and control warfare (IO/C2W) support to the land components and Army commands to facilitate planning and execution of Information Operations. ...."[75], they directly effect the senior Army leadership's observation and orientation steps in the decision cycle. The second criterion is effect on the Army's strategic aims. The domain of information is evident starting with the National Security Strategy. The latest strategy,

dated October 1998 states that it is "US policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on our critical infrastructures, especially our information systems."[76] This is translated within the Army's strategic aims in the third pillar of 'preparing' for the future. The Army's Advanced Warfighter Experiments, Force XXI, and Army After Next initiatives are recent and ongoing vehicles to implement this pillar. The LIWA has been involved in all of these programs as well as conducting both offensive and defensive IO tasks for current operations. IO cells also influence the Army's 'shaping' missions. Numerous articles and lessons learned from the Army's mission in Bosnia credit the IO cell and information operations with being absolutely necessary for the task force to succeed in its 'shaping' mission.[77] The final criterion is impact on combat power. As a combat multiplier within the brigade and division, IO cells orchestrate a synergistic effect from the individual capabilities of IO. An example of this is synchronizing and deconflicting the civil affairs message with messages being prepared for public affairs teams and with the PSYOP plan. A consistent message has a much greater effect. Add to this the complexity of deconflicting an informational deception plan and electronic warfare operations and the effects can be even greater. Negating the enemy's options through a well synchronized deception and informational campaign will increase the ability to mass the division's fires. This has the potential to increase the lethality of the combat power within the division. Therefore, the IO cell can impact on the division's combat power. These IO cells meet all three criteria and are therefore information centers of gravity.

This chapter identified eight key components of information superiority. These components were analyzed using three defined criteria to identify the Army's information

centers of gravity. Two such centers of gravity were identified; the Army commanders and the Army IO cells. Chapter four considers whether the Army can effectively protect these centers of gravity.

Protecting Army Information Centers of Gravity

Thus far, this monograph has identified two information centers of gravity. They are Army commanders and the information operations cells. The term 'Army commanders' refers both to the individuals currently leading the Army and to the system that develops and trains these leaders. Information operations cells includes all levels of these cells from the Land Information Warfare Activity (LIWA) to the ad hoc cells established at division and brigade levels. This chapter answers the final research question - Can the Army defend its information centers of gravity. This chapter considers the answer from two perspectives. First it considers the components of defensive IO and their applicability towards defending the centers of gravity. The components of defensive IO as defined in chapter one are; physical security, OPSEC, counterdeception, counter-PSYOP, counterintelligence, electronic protect (EP), with support from public affairs and civil affairs. Each center of gravity is considered independently using these defensive capabilities. Secondly, the monograph introduces some of the current programs and initiatives being developed for executing defensive IO.

Army Commanders

The primary and most effective protection for Army commanders is physical security. It includes individual awareness for lower level commanders up to dedicated security forces for the highest levels of command. Although these levels of security cannot guarantee safety, they are a deterrent and the security forces are a proven force against conventional small arms attacks. Operations security is another effective

protection tool. OPSEC limits access and supports deterrence. At lower levels of command, OPSEC is an individual responsibility. At higher levels, it expands to include both the dedicated security forces and other personnel that work with the commanders. OPSEC must be balanced with the public affairs component. An effective PA campaign serves to validate and reinforce the competence of the Army's leadership. Expanding General Reimer's credo that 'soldiers are our credentials,' the Army's commanders are credentials for the message that the US Army is a highly skilled and professional organization. This message is also a deterrent against a strike on the Army leadership. Counterdeception does not have wide applicable to protecting the Army's commanders because it is focused on specific enemy deception campaigns. Counter-PSYOP is an effective tool when it is used to counter a belligerent's PSYOP campaign against the US Army leadership. EP is also applicable to protecting the leadership. EP protects the leadership as it protects all aspects of the Army by masking electronic signatures and signals. Counterintelligence also serves to protect the leadership because it is an effective tool to detect and stop a strike before it happens.

Is this protection adequate? Although these measures cannot guarantee the safety of every Army commander, the systems are in place for overall protection. Also, it is key to recall that the definition of Army commanders is not only those individuals currently filling leadership positions, but includes the Army leadership development system that produces these leaders. One of the greatest qualities of the US Army is the depth of soldier capability. No single individual is irreplaceable, and the system is designed for personnel turn-over. The loss of an Army leader to an enemy attack would have an effect, but has never stopped the US Army before, and will not in the future.

Information Operations Cells

The second information center of gravity is IO cells. Before considering the defensive IO capabilities as tools to protect these cells, it is key to recall that the IO cell is the staff agency responsible to plan, coordinate, control and monitor IO for the organization to include the defensive IO capabilities. They are in the position to synchronize their own protection using these capabilities as well as the protection of the remainder of their organization. Because this center of gravity is a physical entity, physical security is the most prominent capability for protection. As with commanders, the level of physical security available is directly related to the location of the cell within the Army architecture. IO cells receive the same level of protection as every other operational staff in the headquarters. They fall under the umbrella of the post, camp or field location security measures which are determined by the commanders. The level of security is determined based on the location of the force, the overall area threat assessment, and the immediate threat assessment based on current events. Establishment of Threat Conditions (THREATCONs) are a command responsibility.

OPSEC is an additional effective tool for protecting these cells. While the mission of IO has received recent attention both in military journals and the press at large, the personnel assigned do not largely receive that attention. As with lower level commanders, OPSEC is a personal responsibility based on the THREATCON and sound judgment. The higher level IO cells, and LIWA in particular, use public affairs techniques to advertise and 'spread the gospel' about their missions. They maintain a publicly accessible web site and are highly publicized in trade and military journals. This public affairs technique can be an effective deterrent by advertising the strengths and

capabilities of the organizations. It is also an effective tool for increasing security by soliciting input from other IO specialists throughout the field. The IO web sites throughout the Department of Defense and civilian corporations are a clearing house for information and techniques for initiating and improving defensive IO capabilities.

Except in extreme and unique circumstances, counterdeception does not provide significant protection for IO cells, but counterintelligence is key to identifying and nullifying threats. Close links between the IO cell and counterintelligence organizations provide an excellent tool for protection of all types of targets to include the cell itself. EP also may protect the IO cell in specific circumstances when an enemy or belligerent's electronic systems are targeting the IO capabilities. Counter-PSYOP as part of a larger PSYOP campaign is another effective defensive IO capability for establishing credible deterrence and civil affairs operations may be used to reinforce the synchronized public affairs and counter-PSYOP messages.

The defined IO defensive tasks provide protection mechanisms for both identified information centers of gravity. Although the levels of protection vary based on numerous factors, the foundation is in place to protect both the Army commanders and the Army's information operations cells from threats from foreign countries.

As stated in the delimiters in chapter one, this monograph does not consider other threats such as hackers, criminals, organized crime and nongovernmental terrorists. The length limitation does not mean to diminish or under emphasize the potential of these threats and they should be considered. Without undertaking that analysis here, it is worthwhile to introduce some of the ongoing initiative to implement defensive IO. In May 1998, President Clinton signed Presidential Decision Directive (PDD) 63. This

directive makes it US policy to take all necessary measures to swiftly eliminate any significant vulnerability to physical or information attacks on our critical infrastructures, especially our information systems."[78] The directive is the authority behind the establishment of the National Infrastructure Protection Center located at the FBI Headquarters. The NIPC is headed by a political appointee with two deputies. One deputy is an employee of the FBI, and the other is representative from the Department of Defense. Along with the mission to protect the real-property infrastructure, the NIPC also protects government operations, telecommunications and banking/financial systems. This charter reaches out to provide protections for STAMIS network systems and other key IO capabilities discussed in chapter three.

Other initiatives have taken place and are ongoing within the Department of Defense. The establishment of the Land Information Warfare Activity, in conjunction with similar joint, air and naval activities, in 1996 has established a single point of contact for information warfare issues. In addition to providing overall guidance for land IO issues, LIWA was also the lead agency in the Army's Red Team Exercises.[79] These exercises are designed to attack a unit's command and control and other information systems during planned tests, exercises and demonstrations. The results from the exercises are used to update and improve defensive IO procedures. The LIWA works for the Army's Deputy Chief of Staff for Operations which provides high visibility for Red Team and other IO issues. It is important to note that it is a 'land' activity, not just an Army agency. In the spirit of true functionality, LIWA includes the Marine Corps in its support activity roles.

In addition to direct threats to information centers of gravity, the other key components of IS must also be protected in order to protect the overall capabilities of the centers of gravity. Examples are the automated networks (C2 and STAMIS) that clearly support the information centers of gravity. To respond to threats against these and other Department of Defense automated systems, the Joint Chiefs of Staff recently agreed to establish a standing joint task force (JTF) for CND (computer network defense). The JTF will be established at the Defense Information Systems Agency (DISA). The JTF will derive its Title 10 command authority directly from the National Command Authorities (NCA), and will be available to be assigned to a unified combatant commander, if required."[80] The other key components have similar protection measures either in place or being initiated as part of the focus on defensive information operations.

This chapter uses the defensive IO capabilities to determine if the Army can effectively protect its information centers of gravity. The determination is that the Army does have the capability and mechanisms to protect its Army commanders and the information operations cells. The chapter also introduces some ongoing initiatives in the realm of defensive IO both within the Department of the Army and within the Department of Defense and federal government as a whole. These efforts and numerous levels require coordination and synchronization to effectively protect both the information centers of gravity and the other key components of information superiority.

Conclusion and Recommendations

Conclusion

This monograph identified two information centers of gravity for the United States Army and determined that the Army does have the capabilities to defend these centers of gravity. The information centers of gravity are the US Army commanders and the IO cells established from brigade-level up to the Department of the Army. The monograph determined that the Army has the defensive IO capabilities necessary to defend these two information centers of gravity.

The methodology employed was sequential using a building-block approach. First the monograph defined the relevant terms using current and emerging doctrine. The monograph used Joint Publication 3-13, <u>Joint Doctrine for Information Operations</u>, and the Integrated Concept Team Draft of FM 100-6, <u>Information Operations: Tactics, Techniques and Procedures</u>, as the source for definitions. These definitions and the works of Brigadier General Wayne Hall (USA), Colonel John Boyd (USAF), and Lieutenant Commander Jeffrey Harley (USN) were then used to validate the term 'information centers of gravity'. The monograph also used current terminology to identify eight key components of information superiority. They are; adversary intelligence, friendly/operational intelligence, Army commanders, strategic C2 networks, other strategic networks, tactical networks, data storage facilities, and IO cells.

Three criteria were established to analyze these components and determine if any are information centers of gravity. The criteria are: influence on the Army decision cycles; effects on the Army's strategic aims; and impact on the Army's combat power.

Using these criteria, the two information centers of gravity were identified. A second analysis used the defined defensive IO capabilities to determine if the Army can protect these centers of gravity. The analysis determined that the Army does have the means necessary to protect them. Finally, the monograph introduced some ongoing programs and projects to assist in protection of all facets of IO at the Army, DoD, and federal government levels.

Recommendations

This monograph was limited by both length and classification. The analysis introduced here should be continued to include threats other than foreign governments. Hackers, terrorists, industrial espionage, insiders, and other criminals were not considered. The analysis here should be expanded to consider these threats. It should also be expanded to consider the information centers of gravity for the Department of Defense. Additionally, initiatives are underway within the federal government through the National Infrastructure Protection Center to protect the US government operations, emergency services, gas/oil storage and delivery, water systems, banking systems, electrical energy, transportation and telecommunications. These areas should be expanded and analyzed to determine the national information centers of gravity. Once identified, they should be assessed to locate and mitigate any vulnerabilities. Additionally, the DoD and Department of the Army information centers of gravity should be reviewed to make sure that they are not contradictory to the federal government's centers of gravity. While it is wrong to assume that they should be the same at every level, they should not contradict each other.

Appendix A, Tables

SERVICE (source)	DEFINITION
Joint Doctrine (JP 1-02)	Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength or will to fight.[81]
Army (FM 101-5-1)	The hub of all power and movement, on which everything depends.[82]
Navy (NDP 1)	That characteristic, capability, or location from which the enemy and friendly forces derive their freedom of action, physical strength or will to fight.[83]
Air Force (AFDD 1)	Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength or will to fight.[84]
Marine Corps (FMFM 1)	Critical Enemy Vulnerabilities[85]

Table A-1, US Military Definitions of Center of Gravity

CAPABILITY	RESPONSIBLE ORGANIZATION
EW	Military Intelligence Organizations (Orgs.)
PSYOP	Psychological Operations Orgs.
Counterdeception	Military Intelligence Orgs.
CI	Military Intelligence Orgs.
CNA	Special Compartmented Services (classified)
PA	Public Affairs Orgs.
CA	Civil Affairs Orgs.

Table A-2, Responsibilities for IO Capabilities

KEY COMPONENTS
Adversary Intelligence
Friendly/Operational Intelligence
Army Commanders
Strategic C2 Networks
Other Strategic Networks
Tactical Networks
Data Storage Facilities
IO Cells

Table A-3, Key Components of Information Superiority

Endnotes

[1] Joint Pub 3.13, <u>Joint Doctrine for Information Operations</u>, (Washington DC, Government Printing Office, 9 October 1998) I-1.

[2] FM 100-6, <u>Information Operations: Tactics, Techniques and Procedures</u>, (Integrated Concept Team Draft) (June 1998), 1-10.

[3] Wayne M Hall, BG. *Reflections on 21st Century Information* Operations, Paper dated 2 January 1999, published on the internet at www.dami.army.pentagon.mil/creative_ideas/main.html, 9.

[4] Ibid.

[5] FM 100-1-5, <u>Operational Terms and Graphics</u>, (Washington DC, Government Printing Office, 30 September 1997), 1-125.

[6] Random House Dictionary, 2nd edition, Random House Inc. (New York, NY, 1987) 1553.

[7] Carl von Clausewitz, <u>On War</u>, ed. and trans. Michael Howard and Peter Paret, (Princeton NJ: Princeton University Press, 1976) 595-596.

[8] BCTP Information Operations Workshop briefing slides, dated Jan 99, Battle Command Training Program, Ft Leavenworth, KS.

[9] CGSC Course Information Operations class notes dated March 98, Command and General Staff College, Fort Leavenworth, KS.

[10] FM 100-6 (D), 1-12 and 1-13.

[11] Ibid. 1-13.

[12] Ibid. 1-14.

[13] FM 100-6 (D), 1-10.

[14] Joint Pub 3-13, vii.

[15] FM 100-6 (D), 4-2 and Joint Pub 3-13, viii.

[16] Special IO is included in the doctrinal definition, however it is beyond the scope of this monograph and will not be discussed. According to Joint Pub 3-13, SIO "are information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the US, required a special review and approval process (JP 3-13, page I-11). The delimiters section of Chapter 1 of this monograph exempts SIO from the scope of this paper.

[17] Joint Pub 3-13, viii.

[18] Christopher Bassford, <u>Clausewitz in English, The Reception of Clausewitz in Britain and America 1815-1945</u>. (Oxford, England, Oxford University Press, 1994), 11.

[19] Carl von Clausewitz, 595-6.

[20] COL John A Warden III, USAF, "The Enemy As a System", *Airpower Journal*, Spring 1995, 49. COL Warden identifies today's enemies as complex systems with five rings of "centers of gravity." The enemy can be defeated by striking the center ring - command and control - or by indirectly striking the system by destroying elements of the outer rings. Throughout his article, he equates a center of gravity with a vulnerability that can be destroyed either directly or indirectly to defeat the enemy.

[21] Ibid. 48-55. The five rings at the strategic level are: leadership, organic essentials, infrastructure, population and the fielded military. At the operational level, they are: the commander; organic essentials - logistics; infrastructure - roads, airways, seaways, rail, lines of communications; support personnel; and field forces - aircraft, ships and troops.

[22] Carl von Clausewitz, <u>On War</u>, quotes from pages 486 and 597 and explained by David S. Fadok, in his monograph *John Boyd and John Warden, Air Power's Quest for Strategic Paralysis*, (Maxwell Air Force Base, Alabama: Air University Press, February 1995) footnote 4, page 16.

[23] Wayne M. Hall, p. 9.

[24] Joint Publication 1, <u>Joint Warfare in the US Armed Forces</u>, (Washington DC, 11 November 1991) pages 21-22 and 39.

[25] Wayne M. Hall, p. 22.

[26] Jeffrey A. Harley, Lieutenant Commander, USN, "Information, Technology, and the Center of Gravity", *Naval War College Review*, (Winter 1997, vol. L, No. 1) 67.

[27] Ibid. 78.

[28] David S. Fadok, 15.

[29] Joint Pub 3-0, III-21.

[30] Joint Pub 3-13, viii.

[31] FM 34-1, 7-2.

[32] Defensive IO is defined on page 1-13 of FM 100-6 (D), Information Operations: Tactics, Techniques, and Procedures as "the integration and coordination of policies and procedures, operations, personnel, and technology to protect information and defend information systems. Defensive IO are conducted through information assurance, physical security, OPSEC, counter-deception, PSYOP, counterintelligence, electronic warfare, and special information operations. Defense IO ensures timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."

[33] FM 100-6 (D), 1-28.

[34] Office of the Joint Chiefs of Staff Joint Electronic Library, JP 1-02, Department of Defense Dictionary of Military and Associated Terms, (Washington DC, June 1998), 343.

[35] Although initially defined in the Office of the Joint Chiefs of Staff Joint Electronic Library's JCS Pub 1-02, Department of Defense Dictionary of Military and Associated Terms dated June 1998, it is also accepted by Army doctrine as the definition for deception. See AR 310-25, Dictionary of United States Army Terms, or FM 90-2, Battlefield Deception, for the same definition with reference back to JCS Pub 1-02.

[36] JP 3-13, GL-5.

[37] FM 33-1, 2-3.

[38] Army Regulation (AR) 10-5, Headquarters, Department of the Army, (Washington DC, Government Printing Office, 30 November 1992) 25.

[39] FM 33-1, Intelligence and Electronic Warfare Operations, (Washington DC, Government Printing Office, 27 September 1994) 5-1.

[40] Ibid. 5-6/5-7.

[41] Ibid. 4-1.

[42] FM 101-5-1, 1-40.

[43] FM 34-1, Intelligence and Electronic Warfare Operations, (Washington DC, Government Printing Office, 27 September 1994) 2-5/2-6.

[44] FM 34-10, Division Intelligence and Electronic Warfare Operations (Washington DC, Government Printing Office, November 1986), iv and 1-1/1-3.

[45] FM 34-1, Intelligence and Electronic Warfare Operations (Washington DC, Government Printing Office, 28 September 1992) 2-20.

[46] Ibid. 2-22.

[47] Joint Pub 1-02, 30.

[48] FM 46-1, Public Affairs Operations, (Washington DC, May 1997) 7.

[49] FM 41-10, Civil Affairs Operations, (Washington DC, 11 January 1993) 1-1.

[50] Ibid. 1-4 and 4-7.

[51] COL Boyd never published his OODA loop theory but included it in a 13 hour briefing titled "Discourse on Winning and Losing" that was presented throughout the Department of Defense. His theories and research have been captured in several articles to include: "Genghis John" by Franklin C. Spinney that was published in The US Naval Institute's Proceedings, in July 1997 just after COL Boyd's death. Spinney worked with COL Boyd for over 23 years. Additionally, MAJ David S. Fadok, USAF includes a detailed analysis of Boyd's OODA loop theory in his School of Advanced Air Power theses titled John Boyd and John Warden, Air Power's Quest for Strategic Paralysis, dated February 1995 and published by the Air University Press at Maxwell Air Force Base, Alabama.

[52] United States Army Posture Statement FY00, America's Army- Assuring Readiness for Today and for the 21st Century, (Washington DC, Government Printing Office, February 1999) 4.

[53] Posture Statement FY00, 5.

[54] FM 100-5, 2-11.

[55] FM 71-100, Division Operations, (Washington DC, Government Printing Office, 28 August 96) 1-1.

[56] Department of the Army Pamphlet 10-1, Organization of the United States Army, (Washington DC, Government Printing Office, 14 June 1994) 31.

[57] Posture Statement FY00, 56.

[58] FM 34-1, 1-1.

[59] Ibid. 2-3.

[60] FM 100-6 (D), 1-46.

[61] FM 100-5, 2-14.

[62] Ibid. 2-15.

[63] Joint Pub 3-13, Joint Doctrine for Information Operations, includes an entire section on IO Responsibilities. The statement in this document is a selected summary of the responsibilities listed for the Chairman, JCS, combatant commanders, chiefs of services, and DoD directorate chiefs.

[64] Tony Loop and William Clingempeel, "An overview of the Warfighter Information Network," Army Communicator, Ft Gordon, GA, US Army Signal Center, Fall 1996, Vol. 21 No. 4) 4.

[65] Government Accounting Office (GAO), "Defense Networks - Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals," (Washington DC, Govmnt Accounting Office, July 1998) 6.

[66] Posture Statement FY00, 44.

[67] GAO, "Defense Networks," 1.

[68] FTS2000 is the Federal Telecommunications System program (2000 refers to the calendar year) that provides long-distance telephone and other telecommunications service for the federal government. Department of Defense agencies are required to use FTS2000 services for all telecommunications services that are not considered vital for command and control purposes. Currently all CONUS routine long-distance telephone services as well as some non-vital long distance special circuits are provided under the FTS2000 contract. It is serviced by the United States Government's General Services Administration.

[69] Heike Hasenauert, "Sharing the Army with the World," Soldiers, The Official US Army Magazine, (Ft. Belvoir, VA, US Army Distributions Operations Facility, March 1999) 43.

[70] JP 3-13, II-5/II-6.

[71] FM 100-6 (D), 2-4.

[72] JP 3-13, IV-3.

[73] Ibid. IV-6.

[74] FM 100-5, 2-11.

[75] LIWA Mission Statement 99, In Addition LIWA will coordinate with national, Joint, and Service IW/C2W centers in the exchange and sharing of intelligence and information support. LIWA provides Field Deployment Teams to support Land Component Commanders.

[76] The White House, "A National Security Strategy For A New Century", (Washington DC, The White House, October 1998) 20-21.

[77] David L. Grange and James Al Kelley, "Information Operations for the Ground Commander," Military Review, (Washington DC, Department of the Army, March-April 1997) 5-12.

[78] National Security Strategy, 20-21.

[79] Clarence A. Robinson Jr., "Rapid Technology Growth Spawns Land Information Warfare Activity," Signal, AFCEA's International Journal, (Fairfax, Virginia, July 1996) 52.

[80] LCDR Andy Wilde, USN, J-39, Joint Staff. "Update: Information Operations" A Common PERSPECTIVE, USACOM Joint Warfighting Center's Newsletter, (Washington DC, Government Printing Office, October 1998, Volume 6, No. 2) 9.

[81] Joint Pub 1-02, 67.

[82] FM 101-5-1, 1-24.

[83] Naval Publication 1, Naval Warfare, 72.

[84] Air Force Doctrine Document 1, Air Force Basic Doctrine, 79.

[85] Fleet Marine Field Manual 1, Warfighting, footnote 28, page 85. Rather than use the term 'center of gravity, the Marine Corps uses the term 'critical enemy vulnerabilities.' They define this term as follows: "Sometimes known as the center of gravity. However, there is a danger in using this term. Introducing the term into the theory of war, Clausewitz wrote "A center of gravity is always found where the mass is concentrated most densely. It presents the most effective target for a blow; furthermore, the heaviest blow is that struck by the center of gravity." Clearly, Clausewitz was advocating a climactic test of strength against strength 'by daring all to win all." This approach is consistent with Clausewitz's historical perspective. But we have since come to prefer pitting strength against weakness. Applying this term to modern warfare, we must make it clear that by the enemy's center of gravity we do not mean a strength, but rather a critical vulnerability."

BIBLIOGRAPHY

Articles

Adams, Thomas K. "Radical Destabilizing Effects of New Technologies," *Parameters: US Army War College Quarterly*. Autumn 1998.

Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force," *Naval War College*, Department of the Army. Spring 1998, 7-19.

Barrows, Tom. "Information Operations," *A Common Perspective*. March 1997, (Vol. 5, num. 1).

Barwinczak, Patricia "Achieving Information Superiority," *Military Review*. Department of the Army. Sept-Nov 1998, No 5.

Boorda, Jeremy M., "Leading the Revolution in C4I," *Joint Forces Quarterly*, Autumn 1995.

Boyd, John R. "Destruction and Creation," 3 September 1976. Reprinted by the Center for Army Tactics, *Foundations of Military Theory*. U.S. Army Command and General Staff College, AY 86/87.

Brewin Bob and Heather Harreld. "DOD Adds Attack Capability to Infowar," *Federal Computer Week Magazine*, 2 March 1998.

Bunker, Robert J. "Information Operations and the Conduct of Land Warfare," *Military Review*. Department of the Army. Sept-Nov 1998, No 5.

Carver, Curtis A. Jr. "Information Warfare: Task Force XXI or Task Force Smith?" *Military Review*. Department of the Army. Sept-Nov 1998, No 5.

Correll, John T., Editor in Chief "War in Cyberspace," Air *Force Magazine*, January 1998.

Debbin, Alan W. "Disabling Systems: War Fighting Options for the Future," *Airpower Journal*, Spring 1993.

De Caro, Chuck. "Softwar," *AFCEA Anthology of Information Warfare*, April 1996.

Dubik, James M. "Military Force: Preparing for the Future," *Military Review*, Department of the Army. March 1992.

Dubik, James M. and Gordon R. Sullivan. "War in the Information Age," AUSA Institute of Land Warfare Landpower Essay Number 94-4. May 1994.

Dunlap, Charles J. Jr. "21st-Century Land Warfare: Four Dangerous Myths," *Parameters: US Army War College Quarterly*. Autumn 1997.

Echevarria, Antulio J. II "Tomorrow's Army: The Challenge of Nonlinear Change,"
    Parameters: US Army War College Quarterly. Autumn 1998.

Grange, David L. and James A. Kelley. "Information Operations for the Ground
    Commander," *Military Review*, Department of the Army. .March-April 1997, 5-12.

Gumahad, Arsenio T. "The Profession of Arms in the Information Age," *Joint Force
    Quarterly.* Spring 1997.

Hall, Wayne M. "Reflections on 21st Century Information Operations," Unpublished
    Paper, 2 January 1999.

Hasenauert, Heike. "Sharing the Army with the World," *Soldiers, The Official U.S. Army
    Magazine*, US Army Distributions Operations Facility, March 1999.

Henry, Ryan and C. Edward Peartree "Military Theory and Information Warfare,"
    Parameters: US Army War College Quarterly. Autumn 1997.

Libicki, Martin C. "Information War, Information Peace," *Journal of International
    Affairs,* Spring 1998, 411-428.

Loop Tony and Clingempeel, William. "An Overview of the Warfighter Information Network,"
    Army Communicator. Fall 1996, Vol. 21 No. 4.

Mahnken, Thomas G. "War in the Information Age," *Joint Force Quarterly.* Winter 1995-96.

Mendel, William W. and Tooke, Lamar "Operational Logic: Selecting the Center of Gravity."
    Military. Department of the Army. June 1993.

Metz, Steven. "Which Army After Next? The Strategic Implications of Alternative Futures,"
    Parameters: US Army War College Quarterly. Autumn 1997.

Nelson, Bradford K. "Applying the Principles of War in Information Operations," *Military
    Review.* Department of the Army. Sept-Nov 1998, No 5.

Robinson, Clarence A. "Army Information Operations, Protect Command and Control,"
    Signal, AFCEA's International Journal. July 1996.

Robinson, Clarence A. "Rapid Technology Growth Spawns Land Information Warfare Activity,"
    Signal, AFCEA's International Journal. July 1996.

Schnieder, James J. "Black Lights: Chaos, Complexity, and the Promise of Information
    Warfare," *Joint Force Quarterly.* Spring 1997.

Spinney, Franklin C. "Genghis John," *U.S. Naval Institute Proceedings.* July 1997,
    Volume 123/7/1,1313.

Struble, Dan. "What Is Command and Control Warfare?" *Naval War College Review.* Naval War College. Summer 1995.

Van Riper, Paul K. "Information Superiority," *Marine Corps Gazette*, June 1997.

Warden, John A. COL. "The Enemy As A System," *Airpower Journal*, Spring 1995.

Washington, Douglas W. "Onward Cyber Soldiers," *Time Magazine*, 21 August 1995, Volume 146, No. 8.

Wilde, Andy. "Update: Information Operations, *A Common PERSPECTIVE, USACOM Joint Warfighting Center's Newsletter.* October 1998, Volume 6, No. 2.

Books

Alberts, Davis S. The Unintended Consequences of Information Age Technologies: Avoiding the Pitfalls, Seizing the Initiative. Washington D.C.: National Defense University, April 1996.

Bassford, Christopher. Clausewitz in English, The Reception of Clausewitz in Britain and America 1815-1945. Oxford England: Oxford University Press, 1994.

Clausewitz, Carl von. On War. Princeton, NJ, Princeton University Press, 1976.

Dunnigan, James F and Albert A. Nofi. Victory and Deceit - Dirty Tricks at War. New York New York, William Morrow and Company Inc., 1995.

Kelly, Kevin. Out of Control, The New Biology of Machines, Social Systems and The Economic World. Reading, Massachusetts: Addison-Wesley Publishing Company, 1994.

Kuo, T.W. ed. Sun Tzu: Manual for War. Chicago, Illinois: Alti Press, 1989.

Libicki, Martin C. Defending Cyberspace and Other Metaphors. Washington D.C.: National Defense University, 1997.

Libicki, Martin C. What is Information Warfare? Washington D.C.: National Defense University, 1995.

Libicki, Martin C. and Jack Nunn and Bill Taylor. US Industrial Base Dependence/ Vulnerability. Washington D.C.: National Defense University's Mobilization Concepts Development Center, Institution for National Strategic Studies, 1995.

MacGregor, Douglas A. Breaking the Phalanx: A New Design for Landpower in the 21st Century. Westport, CT: Praeger Publishers, 1997.

McKnight, Clarence E. ed. Control of Joint Forces: A New Perspective. Fairfax, Virginia: AFCEA International Press, 1989.

Nichiporuk, Brian and Carl H. Builder. Information Technologies and the Future of Land Warfare. Santa Monica, CA: Rand Arroyo Center, 1995.

Science Applications International Corporation. Planning Considerations for Defensive Information Warfare – Information Assurance. Washington D.C., 1993.

Schwartzstein, Stuart J. D. ed. The Information Revolution and National Security: Dimensions and Directions. Washington D.C.: The Center for Strategic and International Studies, 1996.

Toffler, Alvin. Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century. New York: Bantam Books, 1990.

Toffler, Alvin and Heidi Toffler. War and Anti-War: Survival at the Dawn of the Twenty-First Century. Boston: Little, Brown and Company, 1993.

Turabian, Kate L. A Manual for Writers of Term Papers, Theses, and Dissertations. 6th ed., Chicago, IL: The University of Chicago Press, 1996.

Tzu, Sun. The Art of War. trans. by Griffith, Samuel B. London, England: Oxford University Press, 1963.

Van Creveld, Martin. Command in War. Cambridge, MA: Harvard University Press, 1985.

Manuals/Government Documents

United States Congress. Title 10, US Code. Washington D.C.: Government Printing Office, 1 January 1997.

United States General Accounting Office Report to the Ranking Minority Member, Committee on Govenmental Affairs, U.S. Senate. DEFENSE NETWORKS - Management Information Shortfalls Hinder Defense Efforts to Meet DISN Goals. Washington D.C.: General Accounting Office, July 1998.

Office of the Joint Chiefs of Staff. Information Warfare - A Strategy for Peace ... The Decisive Edge in War. Washington D.C.: Government Printing Office, undated.

Office of the Joint Chiefs of Staff. Joint Pub 1-02, DOD Dictionary of Military and Associated Terms. Washington D.C.: Government Printing Office, June 1998.

Office of the Joint Chiefs of Staff. Joint Pub 3-13, Joint Doctrine for Information Operations. Washington D.C.: Government Printing Office, 9 October 1998.

Office of the Secretary of Defense. Information Warfare – Defense. Washington D.C.: Government Printing Office. 1996.

US Department of the Army, <u>Department of the Army Pamphlet 10-1, Organization of the United States Army</u>. Washington D.C.: Goverment Printing Office, 14 June 1994.

US Department of the Army, <u>Army Regulation 10-5, Headquarters, Department of the Army</u>. Washington D.C.: Goverment Printing Office, 30 November 1992.

US Department of the Army. <u>FM 33-1, Psychological Operations</u>. (<u>Fleet Marine FM 3-53</u>). Washington D.C.: Government Printing Office, 18 February 1993.

US Department of the Army, <u>FM 34-1, Intelligence and Electronic Warfare Operations</u>. Washington D.C.: Government Printing Office, 28 September 1994.

US Department of the Army, <u>FM 34-10-2, Intelligence and Electronic Equipment Handbook</u>. Washington D.C.: Government Printing Office, 13 July 1993.

US Department of the Army, <u>FM 34-8, Combat Commander's Handbook on Intelligence</u>. Washington D.C.: Government Printing Office, 28 September 1992.

US Department of the Army, <u>FM 41-10, Civil Affairs Operations</u>. Washington D.C.: Government Printing Office, 11 January 1993.

US Department of the Army, <u>FM 16-1, Public Affairs Operations</u>. Washington D.C.: Government Printing Office, May 1997.

US Department of the Army, <u>FM 71-100, Division Operations</u>. Washington D.C.: Government Printing Office, 28 August 1996.

US Department of the Army, <u>FM 90-2, Battlefield Deception</u>. Washington D.C.: Government Printing Office, October 1988.

US Department of the Army, <u>FM 100-5, Operations</u>. Washington D.C.: Government Printing Office, 19 January 1993.

US Department of the Army, <u>FM 100-5 Operations</u> (draft). Washington D.C.: Government Printing Office, June 1998.

US Department of the Army, <u>FM 100-6, Information Operations</u>. Washington D.C.: Government Printing Office, 6 December 1995.

US Department of the Army, <u>FM 100-6, Information Operations: Tactics, Techniques, and Procedures</u> (Integrating Concept Team Draft). Washington D.C.: Government Printing Office, June 1998.

US Department of the Army, <u>FM 100-15, Corps Operations</u>. Washington D.C.: Government Printing Office, 29 October 1996.

US Department of the Army, <u>FM 101-5, Staff Organization and Operations</u>. Washington D.C.: Government Printing Office, 31 May 1997.

US Department of the Army, EM 101-5-1, Operational Terms and Graphics. Washington D.C.: Goverment Printing Office, 30 September 1997.

US Department of the Army, United States Army Posture Statement FY00, America's Army - Assuring Readiness for Today and for the 21st Century. Washington D.C.: Goverment Printing Office, February 1999.

US Department of the Army, Information Operations Division. Information Operations: A Strategy for Victory through Information Dominance. Washington D.C.: Government Printing Office, 1995.

Monographs and Thesis

Fadok, David S. "John Boyd and John Warden: Air Power's Quest for Strategic Paralysis." School of Advanced Air Power Studies Theses. Maxwell Air Force Base, Alabama: Air University Press, February 1995.

Nowowiejski, Dean A. "Concepts of Information Warfare in Practice: General George S. Patton and the Third Army Information Service, August-December 1944." School Of Advanced Military Studies Monograph. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 1995 (ADA 301 155-4).

Phillips, Gary E. "Information Operations – A New Tool for Peacekeeping" School Of Advanced Military Studies Monograph. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 1997 (ADA 331 354-2).

Smith, Kevin B. "The Crisis and Opportunity of Information War" School of Advanced Military Studies Monograph. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 1994 (ADA 284 756-5).

Stoner, John K. "Energizing the Trinity: Operational Implications of Warfare in the Age of Information Technology" School of Advanced Military Studies Monograph. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 1993 (ADA 274-442-5).

Uchida, Ted T. "Building A Basis for Information Warfare Rules of Engagement" School Of Advanced Military Studies Monograph. Fort Leavenworth, Kansas: U.S. Army Command and General Staff College, 1998. (ADA 340 230-4).