STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: IS THE ARMY DOING ENOUGH?

BY

COLONEL CHARLES M. BORG
United States Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

INFORMATION OPERATIONS: Is the Army Doing Enough?

by

Colonel Charles M. Borg
U.S. Army

Colonel Kevin R. Cunningham
Project Advisor

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

ABSTRACT

AUTHOR: Colonel Charles M. Borg

TITLE: INFORMATION OPERATIONS: Is the Army Doing Enough?

FORMAT: Strategy Research Project

DATE: 01 April 2001 PAGES: 51 CLASSIFICATION: Unclassified

For ten years the Department of Defense (DOD) and the Army have addressed information operations. Over the centuries militaries have conducted operations we today call information operations. In many respects the United States is the most prolific user of information operations while simultaneously it is most susceptible to them. For the U.S. to remain a world superpower and to ensure national security it must be preeminent in information operations. The Army, as a leader in information operations and a significant member of the national security establishment, must continue to improve its information operations capabilities. The Army's execution of information operations must and will tremendously reduce the potential for the United States to be strategically disadvantaged and should contribute significantly to its strategic advantage.

United States Armed Forces will conduct operations under conditions of information superiority. Historically, the Army has conducted operations that today are considered information operations. This paper asks the question, is the Army doing enough to ensure its necessary and appropriate contribution in information operations? It provides background on DOD And Army information operations development and identifies shortfalls in current Army doctrine and training. The discussion ends with recommendations for improvements to the shortfalls identified.

TABLE OF CONTENTS

INFORMATION OPERATIONS: IS THE ARMY DOING ENOUGH?

> Currently, there is a considerable debate throughout the United States Armed Forces concerning information operations. Some herald it as a new form of warfare, driven by technology and globalization; others see it as an enabling function the United States Armed Forces have conducted throughout their history and therefore nothing new. While both sides agree that there is a requirement for information operations, confusion persists on what exactly is information operations, who conducts it, and how is it integrated into existing and emerging organizations and processes.
>
> —MAJ Charles Eassa, SAMS Monograph

IMPLICATIONS OF INFORMATION OPERATIONS: WHY BOTHER?

The term "information operations" represents a new concept of warfare with technological, doctrinal, and organizational dimensions. The idea of "information operations" emerged from the experience of the Gulf War and a very lively debate within the military affairs community about the implications of information technology for military power.

POTENTIAL OPPORTUNITIES AND VULNERABILITIES

Virtually all the literature on information operations (IO) suggests that the U.S. has dominated the development of IO technologies and IO doctrine. As a result, the U.S. is in a dominant information operations position. Most writers on the subject also agree that the U.S., because of its dependence on its technological advancement, could be exceptionally vulnerable to information operations. For example, David J. Farber, an Internet pioneer who serves on the board of the online civil liberties group, Electronic Frontier Foundation, has observed that

> ...as dependency on the Internet increases, cyberwarriors will do real damage. Businesses will collapse if customers can't reach them online, power grids might be brought down with a mouse click. At some point somebody's going to get the brilliant idea, Why bomb them? Why not cyberbomb them...If war is hell, cyberwar could turn out to be cyberhell.[1]

Although possibly overstated, responsible military planners cannot ignore the implications of Mr. Farber's analysis. Military and other national security planners must develop an effective national security strategy to secure the nation from threats and advance her interests.[2] If Mr. Farber's prognosis is correct, then information operations, and the other informational aspects of national security strategy, are critical to the security of the U.S. because they could affect the commercial, industrial, educational, economic, telecommunications and vital infrastructure that supports U.S. national power.

Just imagine this:

> Things go wrong mysteriously with the computers of the U.S. Defense Department. The President asks if the nation is under attack by an enemy and by who might it be. The top experts confess, We just don't know...information warfare is still imprecisely defined, but it basically refers to an attack on information-based resources, such as complex management systems and infrastructures involving control of electric power, money, air traffic, etc.[3]

VALUE OF INFORMATION OPERATIONS

It is clear that information operations are becoming an ever more a significant aspect of military operations. The capability to successfully conduct information operations is also becoming a key component of U.S. military strategy. For the U.S. military to fail to achieve and maintain dominance in this arena will certainly place the U.S. at a significant strategic disadvantage. In recognition of this possibility, the Joint Staff published Joint Vision 2020 (JV 2020). This document provides a vision of future war and of a corresponding American military strategy that is enabled by its information resources. Joint Vision 2020 outlines specific aspirations for the military services as a way to synchronize their efforts in the information operations field and other aspects of precision warfare.[4]

The Army has also been involved in the continuing dialogue about the implications of information operations and has undertaken a number of doctrinal, technological, and organizational initiatives to improve and expand its information operations capabilities consistent with JV 2020. The Army has a responsibility to ensure that it has a sensible and effective conceptualization of information operations and that this concept is translated into meaningful doctrine, effective organizations, and where appropriate, capable weapons. The Army must also be able to conduct information operations as part of a joint/combined force, or unilaterally if necessary. To this end the Army has taken several reasonable steps, given the complexities of this new field, towards developing capabilities that will contribute to dominance in the information operations field. These steps pertain to doctrine, personnel management, training, research, development, test and evaluation, and the fielding of equipment.

Briefly summarized, these steps include the publication of an initial Field Manual on the subject and the drafting of an updated version of the manual in keeping with emerging joint doctrine. The Army also created the Land Information Warfare Activity (LIWA) as a focal point for the development and fielding of these capabilities. In the personnel field, the Army created the Functional Area (FA) 30 Information Operations Officer career field in the Army Officer Personnel Management System (OPMS). The Army also continues a number of research and

development programs with the potential of fielding "weapons" that have effects consistent with information operations aspirations.

While the Army has made progress to date, it is important that we examine whether the Army has gone far enough and fast enough in its development of information operations capabilities to fulfill the Army's role as envisioned in JV 2020. The purpose of this paper is to address this question and provide recommendations to enhance the continuing development of information operations in the Army. An integral function of this process is to specifically identify those aspects of Army Information Operations in which development is too slow and or lacking sufficient detail, focus and vision for success. The implementation of these recommendations will help ensure that the Army is fully capable of supporting its requirements and fulfilling its role in JV 2020.

GENEALOGY OF INFORMATION OPERATIONS

Although a new concept, information operations has a traceable genealogy that includes many elements that have been employed in military operations for decades, if not centuries. Physical destruction, electronic warfare (EW), and psychological operations (PSYOP), for example, are quite traditional, while others, such as computer network attack (CNA), are relatively new.

> During armed conflicts, military forces have used information technologies to accomplish lawful military objectives, citing radio-frequency jamming and electronic countermeasures as examples of the application of information technology to military operations with relatively lengthy historical roots. Today, ... military forces around the world use the latest information technologies, including computerbased systems and datalinks, to conduct their operations.[5]

Some information operations capabilities, such as deception, have a lineage that goes back to the dawn of warfare. For example, Sun Tzu, the ancient military philosopher, noted that:

> All warfare is based on deception. Therefore, when capable, feign incapacity; when active, inactivity. When near, make it appear that you are far away; when far away, that you are near. Offer the enemy a bait to lure him; feign disorder and strike him. When he concentrates, prepare against him; where he is strong, avoid him. Anger his general and confuse him. Pretend inferiority and encourage his arrogance.[6]

In recent decades, military organizations throughout the world have realized the potential value of electronic warfare and jamming. Similarly, great commanders have used psychological operations and deception for centuries.

What is different about the current period, which some commentators have called the Revolution in Military Affairs (RMA), is the belief that much more sophisticated information operations capabilities can and should be developed. To realize this potential – as it is articulated in JV 2020 – the Army must train soldiers to plan, coordinate and execute information operations using the current suite of information operations capabilities while it simultaneously develops new capabilities. The Army must train leaders to know, understand, and integrate information operations first into their thought process and then into the planning and execution of operations.

At the same time that the Army has been contending with information operations, it has embarked on a very broad-based process of "transformation" which will produce new operational doctrine, fighting formations, and enabling technologies. The "transformation" effort will encapsulate many of the information operations initiatives. However, as will be demonstrated, considerable attention must also be given to the synchronization of transformation related changes with those required to fulfill the aspirations of Joint Vision 2020.

The next section of the paper will summarize the development of information operations in the Army over the past ten years or so. This will be accomplished with a chronological review of the governing Office of the Secretary of Defense (OSD) and Joint Staff (JS) policy and doctrine publications; and consequent Army publications. As the review of Army publications draws near to the present day, the paper will present the current state of information operations in the Army as articulated in various Army publications. Then it will describe JV 2020 implications for the Army in the realm of information operations. As a point for comparison, this section will also present the approaches that the USAF and US Navy have taken toward information operations.

The paper will then identify the specific challenges facing the Army in the development of its information operations capabilities, and closes with some options and recommendations to improve the situation.

ARMY INFORMATION OPERATIONS

EVOLUTION OF OSD AND JOINT STAFF INFORMATION OPERATIONS POLICY AND DOCTRINE

The Army conceptualization of information operations has evolved within a context defined by Department of Defense (DoD) policy and Joint doctrine. In order to understand how the Army came to develop its version of IO, it is first necessary to understand the changing nature of the DoD policy and joint policy and doctrine for information operations.

1992, DOD Directive TS3600.1, Information Operations

In December 1992, DOD Directive (DODD) TS3600.1 Information Warfare was published. This top-secret document, like most policy documents, only provided general guidance and a definition of information warfare. Even though DODD TS3600.1 introduced the concept of information warfare, this highly classified document's significance was made known only through conferences, studies, and wargames in which its substance became the subject of discussion and action.[7] DODD TS3600.1 was truly a novel thought at the time it was published. Its conceptual focus was on that which we have come to know more recently as computer network attack (CNA). At the time, the extremely high security controls in a new and emerging field tended to limit the dialogue and study of the new concept to those few with the appropriate clearance. Unfortunately, this restricted a broader dialogue and hampered progress in a vital new field.

Although restricted, it did not prevent that dialogue amongst theorists, authors and military thinkers (in and out of the military). Herein lies another problem, the confusion and ambiguity in concepts and definitions of terms used publicly were not often consistent with those used in the classified world. Nonetheless, DOD Directive TS3600.1 was a crucial first step in which, by the end of 1992, DOD initiated the dialogue on the subject of information warfare and computer network attack. Even though it was highly classified, it was an important beginning in that it caused senior officials of the DOD, as well as their interagency counterparts, to start to consider the fact and implications of information warfare and computer network attack.

1993, CJCS Memorandum of Policy 30, Command and Control Warfare

Following publication of the DOD Directive on information warfare, by a short three months, came guidance on a new concept called command and control warfare. In March 1993, Chairman Joint Chiefs of Staff (CJCS) Memorandum of Policy (MOP) 30, Command and Control Warfare[8], was published. The concept advanced in MOP 30 was predicated upon lessons learned from operation DESERT STORM.

Psychological operations (PSYOP), operations security (OPSEC), deception, electronic warfare (EW) and physical destruction of vital command and control nodes were conducted in an ad hoc manner during DESERT STORM. All five of these operations were, and are, well understood by the military. Three of these, psychological operations, operations security and deception, have been considered elements of warfare for centuries. Yet, as late as DESERT STORM, these operations were planned and executed by relatively unknown, small and often isolated teams. To make matters worse, they were not well coordinated amongst themselves,

or into the overall plan. This lack of integration resulted in a lost opportunity to capitalize on the synergistic effects of these elements operating in a thoroughly coordinated, well-planned manner.

Clearly, the intent, or the desired effect, of MOP 30 was to eliminate, or at least minimize, the stovepipe planning and execution of operations of these various command and control warfare (C2W) elements. The expectation was that the various elements of C2W would be integrated in their planning and execution. The anticipated result of this integration was added advantage for U.S. Armed Forces by the magnification of the synergies and relationships of C2W elements when working together.[9]

It is important to note that by early 1994 the DOD had been engaged in the intellectual dialogue and practical development of information warfare and command and control warfare for at least a couple of years. We will see later that this served as a springboard for the Army's development of these concepts, as well as their continued development at the DOD level.

In January 1994 the first significant public DOD explanation of information warfare was provided in the Annual Report to the President and Congress of the Secretary of Defense. Although the Secretary's report did not define information warfare, it stated that information warfare:

> ... consists of the actions taken to preserve the integrity of one's own information systems from exploitation, corruption, or destruction, while at the same time exploiting, corrupting, or destroying an adversary's information systems and, in the process, achieving an information advantage in the application of force.[10]

Although in the early 1990s much of this dialogue and development was severely restricted due to security considerations, the 1994 Annual Report opened the floodgates to all manner of thinker and writer (military and non-military) permitting a much broader exploration of information warfare. It also raised the question of if and when the DOD would make available a formal, clear, unclassified DOD definition of information warfare.

1995, CJCSI 3210.01, Joint Information Warfare Policy

Throughout 1995 the development of the concept of information warfare continued. During this year the Joint Staff recognized that there are multitudes of actions that can be taken to achieve information superiority. This led, among other things, the CJCS to update the concept and clearly define information warfare. In January 1996, CJCSI 3210.01, Joint Information Warfare Policy, defined Information Warfare (IW) as "Actions taken to achieve information superiority by affecting adversary information, information-based processes,

information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks."[11]

Although counterintuitive given the close similarities in title, this document does not supersede TS3600.1. As has been learned over the years, TS3600.1 had more to do with CNA, while this new CJCSI incorporates earlier comments by the Secretary of Defense and the JS definition of information warfare thereby setting the policy stage for joint doctrine that is soon to follow.

1996, Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare (C2W)

Subsequently, Joint Publication (Pub) 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), published in February 1996, introduced the fundamentals of Information Warfare, explained the elements of C2W and defined several terms, to include, C2W, information, information superiority, information system and information warfare. Joint Pub 3-13.1 cast Command and Control Warfare as "an application of information warfare in military operations and is a subset of information warfare."[12] Furthermore, in a move of great consistency, it defined information warfare exactly as the CJCS did in Joint Information Warfare Policy. In this early effort, Joint Pub 3-13.1 defined information superiority as "That degree of dominance in the information domain which permits the conduct of operations without effective opposition."[13]

One might question the long, slow and rather indirect developmental path for joint doctrine in this field. However, it must be recognized that, at this point in time, in terms of military systems and concepts development, the IW, C2W, IO field was very young. In this very new and emergent field, a deliberate and careful approach was under way to develop new doctrine. After approximately four years of dialogue, exercises, and the publication of several policy documents, joint doctrine was finally released in Joint Pub 3-13.1.

1996, Joint Vision 2010

Contributing to the volume of official literature on the subject, even at the risk of adding confusion, the CJCS also published Joint Vision 2010 (JV 2010) in July 1996. It defined "information superiority" as "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[14] Although not exactly the same, this new definition was similar to that in Joint Pub 3-13.1. "Information superiority is the key enabler of the operational concepts of Precision Engagement, Dominant Maneuver, Focused Logistics, and Full Dimensional Protection." The term information superiority, as defined in Joint Pub 3-13.1 and JV 2010, frames a concept that underpins these

key operational concepts of JV 2010. Although the definitions in these two documents (Joint Pub 3-13.1 and JV 2010) are not identical, they are very similar. Moreover, they are applicable to and supportive of the operational concepts introduced in JV 2010.[15]

1996, DOD Directive S3600.1, Information Operations

DODD S3600.1, Information Operations, in December 1996 opened a new phase in information warfare doctrine. This document, classified secret, was afforded much greater dissemination than the top secret version (DODD TS3600.1) released four years earlier. It captured the thinking on information warfare that developed during the ensuing years, to include, information assurance, information operations, and infrastructure protection, concepts not addressed in the earlier version of the directive. As evidenced by the publication of JV 2010, information warfare was beginning to influence strategic thinking.[16]

2000, Joint Vision 2020

In the fall of 2000, Joint Vision 2020 (JV 2020) was published and disseminated new ideas about future war and about information operations. These had a feedback effect on the doctrine development process and also had further implications for military operations. Written by the Chairman for the CINCs, service chiefs, and other stakeholders, JV 2020 is tall on concept and short on detail. The point is that JV 2020 is written strictly as a concept leaving it up to all stakeholders to decipher, understand, interpret and translate into their own policy and doctrine. JV 2020 posits the "state" of information superiority as a necessary condition in which the joint force can achieve full spectrum dominance, leaving it to the services and joint force commanders to determine the "what" and "how" of information superiority. JV 2020 shows some consistency in the definition of terms, as the definition of information superiority is the same in JV 2010 and Joint pub 1-02.

The goal of JV 2020 is for US forces to have the capability to achieve full spectrum dominance. This translates to the ability of US forces, operating unilaterally, and/or in joint, interagency, and/or multinational partnerships to defeat any adversary and control any situation along the continuum of military operations. Access and freedom to operate in all domains – space, sea, land, air and information – is implied by the JV 2020 concept of full spectrum dominance. In JV 2020 the goal of full spectrum dominance is attained by the application of the operational concepts of dominant maneuver, precision engagement focused logistics and full dimension protection. The key point here is that an environment of information superiority will significantly enhance the application of these operational concepts by innovative soldiers and

leaders. A further implication is that information superiority is an always desired, if not (almost) always necessary, precondition for full spectrum dominance. JV 2020 recognizes that:

> Information superiority is transitory in nature and must be created and sustained by the joint force through the conduct of information operations. ...Information superiority provides the joint force a competitive advantage only when it is effectively translated into superior knowledge and decisions ... "decision superiority" – better decisions arrived at and implemented faster than an opponent can react.[17]

As applied in JV 2020, information superiority is an enabler that provides the joint force the environment in which it can attain full spectrum dominance. The implication of JV 2020 is that the Army must be capable of providing information superiority for Army forces and be able to conduct information operations in support of the Joint Force Commander's requirement for information superiority.

Summary of DOD Policy and Joint Staff Policy and Doctrine

As late as February 2000 one can see that JV 2010 continues to guide the thinking of the Department of Defense. Secretary of Defense Cohen stated:

> The QDR [Quadrennial Defense Review] called for a fundamental reshaping of U.S. forces to capitalize on the emerging Revolution in Military Affairs, which emphasizes superior information capabilities and other advanced technologies. ... At the heart of JV 2010 is the ability to collect, process, and disseminate information to U.S. forces, while denying the enemy the ability to gain and use battle-relevant information.[18]

The last sentence of Secretary Cohen's quote does very closely paraphrase the definition of information superiority found in JV 2010. By the fall of 2000, there is some consistency in the definitions of information superiority and information operations.

As the OSD and Joint Staffs developed information operations guidance and joint doctrine, the Army worked the C2W issue and produced service policy and doctrine to keep pace, and to respond to service requirements.

EMERGENCE OF ARMY INFORMATION OPERATIONS DOCTRINE

1995, TRADOC Pamphlet 525-69, Concept For Information Operations

In August 1995 the Army's Training and Doctrine Command (TRADOC) published TRADOC Pamphlet (Pam) 525-69, Concept For Information Operations, one of the Army's earliest publications on the subject.[19] This was a significant first step for the Army.

Although TRADOC pamphlets are not binding on the Army at large, as are Army regulations and field manuals, they are binding on TRADOC centers and schools. They are the

conceptual foundation upon which doctrine, training, and other requirements are to be based. Simultaneously, these pamphlets serve as an intellectual underpinning for the rest of the Army until doctrine is published. One should not read anything into the apparent lag time from the 1992 publication of DOD Directive TS 3600.1 to the publication of TRADOC Pam 525-69. It is reasonable to accept that the Army was engaged in the classified fora noted earlier and that it was familiar with the documents noted above, Information Warfare and Command and Control Warfare. Given this situation, it appears that TRADOC Pam 525-69 is TRADOC's best integration and conceptualization of the subjects.

In this pamphlet, the Army identified winning the information war was one of the five modernization objectives necessary to achieve land force dominance. The term information operations was described as an integrated approach to gaining and maintaining the information the warfighter required to fight and win, while denying the same to adversaries. TRADOC Pam 525-69 outlined IO as an enabling means to implement future Army operations and our warfighting doctrine. It went on to explain that in a force-projection Army, support for warfighting could be provided from as far back as CONUS. This pamphlet clearly recognized that the information age paradigm would change army organizations, doctrine, processes and operations. Moreover, it would change the way wars are fought. Conceptually, this pamphlet identified information as an essential dynamic enabling dominant military power at the strategic, operational, and tactical levels.[20]

With the publication of TRADOC Pam 525-69, the Army discusses and defines three terms: information operations, information warfare (IW) and command and control warfare (C2W). The definition for IW is extracted from the (then) proposed Joint Pub 1-02, and the definition for C2W is extracted from CJCS MOP 30. Further, this Pam includes an explanation taken from DOD Dir TS-3600.1, "C2W is the military strategy that implements information warfare."[21] There are a few points to be made here. To reiterate, this was the Army's first formal conceptualization of a new and emergent field and the Army's role in it. It was expected to inspire critical thinking and discussion on the topic, and was quite successful in that it led to formal doctrinal development. The final point to be made is that it is significant that the Army, utilizing DOD and Joint Staff definitions, potentially reduced confusion and increased mutual understanding of these emerging information operations concepts.

1996, Army Field Manual 100-6, Information Operations

At the same time that the policy and doctrine process was at work at the DOD level, within the Army a similar process was underway to relate information operations to land warfare

doctrine. By late 1995, the Army was working hard on an up-to-date, comprehensive doctrinal manual for information operations. It is more likely than not, that the subject matters experts who wrote TRADOC Pamphlet 525-69 are the same subject matter experts who wrote this new manual.

Information Operations Terms and Concepts

Published in August 1996, Army Field Manual (FM) 100-6, Information Operations, makes an attempt to clarify the confusion surrounding information operations caused by the many and varied terms and their sometimes inconsistent definitions. FM 100-6, Information Operations, remains in force as the current Army doctrinal manual on the subject. The preface indicates that this manual will focus on command and control warfare (C2W), public affairs (PA), and civil affairs (CA). These are longstanding Army capabilities which the Army currently uses to gain and maintain C2 [command and control] as well as information dominance.[22] This new manual is the Army's capstone publication for information operations; it supports the National Military Strategy and explains the fundamentals of IO for the Army. This Army IO doctrine reflects the joint strategy of command and control warfare (C2W), which implements DOD information warfare policy, and it goes beyond. It provides more specifics than the joint strategy does to make it more useful to field commanders. In FM 100-6, the Army defines information operations as:

> Continuous military operations within the MIE [Military Information Environment] that enable, enhance and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; IO include interacting with the GIE [Global Information Environment] and exploiting or denying an adversary's information and decision capabilities.[23]

FM 100-6 identifies activities that support information operations as acquiring, using, protecting, managing, exploiting and denying information and information systems. This new doctrine acknowledges the tremendous growth in information, information systems and information sources and recognizes the implications of the information age. The Army recognizes in FM100-5, Operations, and FM 100-6 that it must, and is, changing the way it operates in the new technological environment.[24]

FM 100-6 is the Army's first effort to provide clear and comprehensive guidance on information operations to the field in the form of a doctrinal manual. In this new and emerging field it serves to reduce the confusion surrounding information operations and information warfare. It provides definitions for several key terms, to include, command and control warfare, information, information age, information databases, information dominance, information

security, information systems, and information warfare. It should be noted that in this manual the Army's definitions of C2W and information warfare are taken from, and thus are identical to, the joint definitions. The material above provides familiarization and background into the conceptual and intellectual underpinnings of the doctrine that defines and drives information operations. Given this background, we will next explore the Army's organizational construct for information operations.

Staff Organization and Responsibilities

Within FM 100-6, the doctrine defining staff responsibilities for IO and the organization of IO staff elements is particularly significant and deserves a detailed analysis. This is the Army's first doctrinal manual on the subject and its first attempt to identify IO staff responsibilities and organization. FM 100-6 takes a broad-brush approach to the doctrinal roles and functions of staff officers as they relate to information operations; in its 150 pages, FM 100-6 uses less than two pages to discuss staff responsibilities and organization for IO. The message (rather loud in retrospect) therein is that:

> Since IO are only one facet of a larger operation, albeit an important one, the J3/G3 is the primary manager of information. He outlines and monitors the performance and responsibilities of the staff in processing information to support IO and knowledge flow. The J3/G3 ensures the staff collects, analyzes, and presents information to that fulfills the CCIR [Commanders Critical Information Requirements].[25]

According to the FM, the J3/G3 will usually designate one individual to be accountable for all IO actions. It further explains that several key staff members participate in IO coordination and integration to include intelligence, signal, fire support, public affairs (PA), civil affairs (CA), electronic warfare (EW), deception, operations security (OPSEC), psychological operations (PSYOP), and logistics personnel. It is clear, even at this early date, that Army doctrine recognizes that IO is a complex undertaking that requires the support and coordination of a significant part of the staff. As recent as January 2000, the Information Operations Team, ODCSINT, HQDA, also recognized that "[H]istorically, the G-3 has had the responsibility for ensuring that all the above listed activities were maximized in their employment..."[26] Having provided some guidance as to the staff responsibility for information operations, FM 100-6 prescribes the organizational structure of and roles and functions of the individual designated by the J3/G3.

According to FM 100-6, an Information Operations Cell would normally be organized to operate in peacetime and in military operations other than war. A notional IO cell consists of soldiers or officers representing these activities or functions: OPSEC, C2W, intelligence, signal,

CA, PA, Land Information Warfare Activity (LIWA) (more on LIWA later), fire support coordinator (artillery), targeting, staff judge advocate; electronic warfare, PSYOP, and deception. Although unstated in FM 100-6, it is assumed that the IO cell will operate under the supervision of the G3, or his 'designated individual'. At some point along the continuum, as engagement moves from peace to war, FM 100-6 suggests it may be more operationally sound to stand up an Information Operations Battle Staff (IOBS). This IOBS is comprised generally the same as the IO Cell with the added presence of the commander, chief of staff, operations officer (G3), intelligence officer (G2) and signal officer.[27]

In retrospect, one might say that as evidenced by the doctrine in FM 100-6, the Army's understanding of and vision for information operations was limited. As a result, the responsibility for information operations was not specifically assigned to an information operations staff officer (expert); it was relegated to an individual designated by the J3/G3. This is unfortunate, but understandable given that the concept of information operations in 1996 was still very new and only beginning to be developed, not only in the Army but also throughout DOD. The issue of responsibility for information operations is one that we will revisit later in this paper. FM 100-6 provides a minimum doctrinal framework for the staff structure for information operations. It also begs the question of training for information operations.

Information Operations Training

The discussion of information operations training in FM 100-6 is extremely limited. It states "[T]he basic task is to train the force on IO, with an initial focus on those personnel responsible for planning and coordinating the individual elements."[28] Although it is noteworthy that information operations training is not altogether ignored in this manual, it is, on the other hand, barely addressed. Clearly, the direction provided is on the right track. Those personnel who will coordinate and plan information operations with representatives of the various IO elements require significant training. It should be noted that it is generally accepted that personnel working in the various elements of information operations are well trained in their disciplines.

FM 100-6 made necessary decisions about IO staff responsibilities and organization. Given the novel nature of IO, it is hardly surprising that the publication of FM 100-6 led to the further debate that revealed concerns about the training and skills that IO experts would need to fulfill the promise of these operations.

2000, FM 3-13, Information Operations: Doctrine; Tactics, Techniques and Procedures

Since its publication in 1996, FM 100-6 has undergone numerous draft revisions, none of which have been approved and published. The latest revision (renumbered FM 3-13 to correspond with the Joint Pub numbering system), dated September 2000, is in final draft. Given the significant impact of continuous change to the concepts of information warfare and information operations at the Joint level and the extremely dynamic nature of the information environment, one might think this is an extraordinarily long wait for an update to the Army's information operations doctrine. Aside from the fact that there is no prescribed timeline in which a field manual must be updated, it is likely that there was debate as to how to relate information operations to information superiority. This was almost certainly exacerbated by doctrinal differences between various TRADOC centers (most probably the Intelligence and Signal centers) charged to provide input to the manual.[29]

To better describe the enhanced content of the manual, the title of the draft successor manual (to FM 100-6, Information Operations) has been changed to Information Operations: Doctrine; Tactics, Techniques and Procedures (TTP). It was also renumbered FM 3-13 to correspond to the Joint Pub numbering system. This is an improvement over previous manuals, as soldiers and leaders using this manual, in a new and complex field, will have at their fingertips not only the doctrine, but also the TTP necessary to execute that doctrine.

Terms and Concepts

As in most of the earlier OSD, Joint Staff and Army publications that discuss C2W and information operations, FM 3-13 uses many of the same terms and concepts. It includes the concept of information as an element of combat power and relates that information superiority is the execution of the information element of combat power. FM 3-13 also incorporates the concept of information operations as one of the contributors to information superiority. This manual separates IO into two components, offensive and defensive IO and indicates that IO is executed using twelve elements and two related activities. The twelve elements of Information Operations are: Counterintelligence, OPSEC, Physical Security, Information Assurance, EW, computer network attack [CNA], Special Information Operations, Physical Destruction, Counter-propaganda, PSYOP, Counter Deception, and Deception. In FM 3-13 the following two elements are considered related activities to Information Operations: Civil Affairs, and Public Affairs.[30]

It should be noted that the following elements of IO found in FM 3-13 were not previously addressed in FM 100-6 as integral elements of IO. These elements are counterintelligence,

information assurance, computer network attack, counter-propaganda and counter-deception. With the exception of computer network attack, these new elements of information operations are also well developed and understood in the Army. "Of all the capabilities and related activities outlined in JP [and FM] 3-13, it is clear that only those relating to Computer Network Operations (CNO) are new. All other components are established, and have clearly delineated and well-defined roles and responsibilities, primarily within the Army."[31] This statement substantiates an earlier assertion that personnel serving in the various elements of information operations are well trained in their disciplines and is important as it relates to a subsequent discussion on training for IO personnel. At this point, the 'new' element of computer network attack needs to be addressed. FM 3-13 defines computer network attack as "operations to disrupt, deny, degrade and destroy information resident in computers and computer networks, or the computers and networks themselves."[32]

This final draft FM is the Army's next step to stay in synchronization with, or perhaps to get ahead of the Joint Staff. Army has renumbered its manuals to match those of Joint Publications. More importantly, in FM 3-13 the Army talks to information superiority in much the same way that it is addressed in Joint Pub 3-13. This is a good thing. FM 3-13 states, "Information superiority is the operational advantage derived from the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Information operations are defined as actions taken to affect adversary, and influence others', decision-making processes, information and information systems while simultaneously protecting one's own. Furthermore, FM 3-13 explains that information operations are shaping operations designed to create and present opportunities for decisive operations.[33] The definitions of information superiority and information operations are now synonymous in the Joint Staff and Army documents. This will provide for a common understanding, and reduced confusion. As doctrine is intended, this should help minimize the fog of war and make more clear the meaning and intent of these terms as they are used.

Staff Organization and Responsibilities

For the first time in Army doctrine, FM 3-13 also prescribes an organizational structure for information operations. Specifically, FM 3-13 indicates that there will be an Information Operations section assigned to the headquarters (HQ) staff at three echelons: Army Service Component Command (ASCC), Corps, and Division. In prescribing the organizational construct and the roles and functions for these IO Sections, FM 3-13 also reinforces the roles and functions previously specified in FM 100-6 for the IO cell within these same HQs. These newly

designed IO Sections are responsible for the planning, preparation, execution and subsequent assessment of information operations.

Interestingly, the construct in FM 3-13 has organized the IO section differently at various echelons. In the ASCC HQ, the IO Section is organized within the Office of the Deputy Chief of Staff for Operations (ODCSOPS). Quite differently, however, at both Corps and Division, FM 3-13 creates a new principal staff officer with responsibility for IO. This new position is the Assistant Chief of Staff (ACoS), G7, Information Operations Coordinator, (IOCOORD). As might be expected, the IO Coordinator is the chief of the IO section and serves as a coordinating staff officer reporting directly to the Chief of Staff. In terms of numbers, FM 3-13 indicates that there will be at least three FA –30 officer positions for the ODCSOPS, ASCC; and, at least six FA-30 officer positions for the OACoS, G7, IOCOORD, at Corps and Division.[34]

Although responsible for the planning, preparation, execution and assessment of IO, the IO section does not execute these functions in isolation. Throughout these processes, the IO section is responsible to assemble the IO cell (noted above in the section on FM 100-6) consisting of subject matter experts of the various elements of IO (OPSEC, deception, EW, etc.) and coordinates its efforts. Functionally, the Chief of the IO section (the IOCOORD at Corps and Division) chairs meetings of the IO Cell and is responsible for the activities of the IO cell. Ultimately, the purpose of the IO cell is to ensure that the capabilities they represent are employed in a fully coordinated manner to maximize IO effects in support of the commander's plan.

I would have expected the IO coordination function to rest with the G3, as it has in the past and as it was documented in FM 100-6, for the reason previously stated. However, this Information Operations Coordinator, G7, on the staff is a more than acceptable, if not a really good, construct for staff organization at Corps and Division. The roles and functions of the Information Operations Coordinator are many and varied; they will require significant training, expertise and fulltime focus that would likely detract from the effectiveness of the already extremely busy G3. However, one weakness of this draft doctrine is a failure to address the competencies and training necessary for those charged to coordinate IO. This will be addressed below.

The Value of FM 3-13

To put this in perspective, one must recognize that the Army developed IO doctrine in response to new and continuously evolving OSD and JS concepts, policy and doctrine. Earlier this paper indicated that the Army's first cut at doctrine in FM 100-6 was not very sophisticated

in terms of operational concepts or in terms of establishing workable staff relationships between the many entities that already have a piece of the IO mission. With FM 3-13 the Army has done a better job and overall this is an important and positive step for the Army. Concepts for IO, with the exception of weaponization (discussed below) are much better developed and the organizational constructs and their implications are about right. These are both satisfactory for the near term.

To put draft FM 3-13 in perspective, it must be remembered that it is the Army's second iteration of a doctrinal manual for information operations.[35] The information operations field is still relatively young and its essence continues to manifest itself in new ways and its implications for relevance in Army operations grow almost on a daily basis. Given the novelty of information operations and the continuing development of OSD and JS concepts, policy and doctrine, FM 3-13 serves to further refine the guidance and provides a reasonable azimuth for the Army in this field.

IO and the Land Information Warfare Activity

In addition to its discussion of the IO organization at the tactical and operational level, FM 3-13 addresses the Army's operational/strategic capability to provide expert information operations support to commanders at all levels. The Land Information Warfare Activity (LIWA) was created to operationalize information operations in the Army. The Army established LIWA in 1995 under the command of the Intelligence and Security Command and placed it under the operational control of the Army Deputy Chief of Staff for Operations and Plans. Similar to the IW centers of other services, the LIWA focuses in two directions, higher and lower. It represents the Army to sister services, DOD agencies and activities, other national agencies and non-government agencies for the purpose of furthering Army IO. Additionally, LIWA serves as the Army's focal point for information operations to all Army organizations and activities, and is tasked, organized, and equipped to provide them IO support. LIWA support comes in many forms, the most prominent of which are field support teams, the Army Computer Emergency Response Team, and IO vulnerability assessment teams.

Field support teams (FSTs) are capable of providing direct support to army service component commands, army force commanders, and corps and divisions. Historically, LIWA FSTs have provided their unique support to units at each of these echelons. LIWA FSTs have the capability to support these commands in planning, preparing, executing and assessing information operations. FSTs deploy worldwide as necessary to provide supported commands

with IO planning, coordination, and IO assessment. These FSTs can be tailored to the mission and actually serve as an augmentation to the command's IO cell.

The Army Computer Emergency Response Team (ACERT) is responsible to prevent, detect, assess and respond to Army information system security incidents. It does so with four regional CERTs located strategically around the world. The ACERT operates continuously. It serves as the focal point with Defense, and other national agencies for the reporting of computer incidents and subsequent responses. If necessary, ACERT personnel can be deployed to assist commands as they respond to computer incidents. The Army has designated the ACERT as the Army component of the U.S. Space Command's Joint Task Force Computer Network Defense.

The IO vulnerability assessment teams (VAT) assess and enhance a command's defensive IO capabilities. The results of VAT operations provide the command with a thorough review of its vulnerabilities to adversary IO attack capabilities. The VAT can and does assist the command with plans for and implementation of security measures to mitigate these vulnerabilities and it suggests efficiencies to enhance the command's defensive IO capabilities. "Blue" and "red" teams conduct VAT operations. Blue teams conduct non-intrusive assessments focusing on information flow and networks to determine extant or potential vulnerabilities and risk levels. Red teams simulate adversary IO capabilities and attacks against friendly information, information systems and decision-making processes. Red teams serve to enhance readiness and also to verify the effectiveness of countermeasures.

Additional LIWA responsibilities include technical support to reprogramming efforts for smart munitions predicated upon worldwide signature information; designation as the Army's functional proponent for military deception; IO combat developments; and, IO simulations analysis.[36]

SISTER SERVICE INFORMATION OPERATIONS

DoD policy, Joint policy and doctrine, and JV 2010 and JV 2020 established goals for all the armed services. The preceding section reviewed how the Army attempted to deal with the emerging and evolving concepts of IO. A similar effort took place in the Air Force and Navy. The experiences of these services in dealing with these concepts reveal some of the same conceptual, doctrinal, and organizational difficulties that the Army experiences.

USAF Information Operations

In the Air Force, as with all the services, the concepts and doctrine for information warfare preceded the development of information operations. Reacting to OSD and Joint Staff guidance

for information warfare (described above), in 1993 the Air Force was the first service to establish an Information Warfare Center. Named the Air Force Information Warfare Center (AFIWC), it was created by the consolidation of the Air Force Cryptologic Support Center and the Electronic Warfare Center. This teaming of intelligence specialists, operators, engineers and computer specialists was intended to permit AFIWC to conduct "Red Team" operations and provide a computer emergency response team (CERT) services aimed to improve network security.

In 1995 the Air Force established its first Information Warfare Squadron (IWS). Its purpose was to protect Air Force computers and communications and assist in infiltrating enemy computer systems. This IWS was assigned to provide support to 9th Air Force and US Central Command. The Air Force plan was to have an IWS in support of each numbered Air Force supporting a regional combatant command.[37] Due to its cost, particularly in manpower, in 1997 the Air Force began to look for alternatives to the IWS. In 1999 the Air Force adopted a new concept for an Information Warfare Flight whose mission is very similar to that of the IWS, but consists of significantly fewer personnel.

The Air Force concept of IO was first articulated in Cornerstones of Information Warfare by the Secretary (SECAF) and Chief of Staff, US Air Force (CSAF) in 1996. This publication was a very visionary and comprehensive piece in which the SECAF/CSAF set the broad policy outline for USAF information operations. Much more than just a think piece, this paper presents the "why now?" of IO. It defined information, IW and IO, spelled out the components of IW, emphasized information attack, included defensive IW, and provided insights and implications for doctrine. Cornerstones defined IW much the same as did the CJCSI 3210.01; the words are different, however, the meanings are very close. More importantly, in this document the SECAF/CSAF vision for IW is quite expansive. It states, "Information, combined with modern information functions, has distinct characteristics that warrant it being considered a realm, just as land, sea, air, and space are realms."[38] In this respect, information is seen as a realm in which dominance will be contested, and in which and from which military power can be employed.

In 1998 Air Force Doctrine Document (AFDD) 2-5, Information Operations, was published. This doctrine considers information superiority an enabling function like air and space superiority. It views information superiority as a synergistic and indispensable component of aerospace power and further views IO as the means to information superiority. Information operations are divided into two categories: information-in-warfare and information warfare. In AFDD 2-5, the Air Force recognized the definition of IO exactly as it is in DODD S3600.1. However, AFDD 2-5 goes on to explain that a more useful working definition of IO would include

the concepts of information-in-warfare and information warfare. Information-in-warfare comprises all those functions, technological or otherwise, that support and enable the planning and execution of operations, such as weather, intelligence, administrative information, navigation, exploitation of information, and dissemination. Information warfare consists of the attack and defend operations including, basically, all the capabilities and operations previously described as elements of Army IO. AFDD 2-5 not only addresses doctrinal terms and concepts, but also IO processes and organizations.[39]

Since AFDD 2-5 was published in 1998, information operations has been the subject of debate in the Air Force between airmen of all ranks. As a result it was recently updated and is in draft form now. It reiterates that although it strongly agrees with joint doctrine for IO at large it differs on two issues, terms and scope. As described above, the Air Force concept of IO is broader in scope than that of Joint doctrine as it incorporates the concepts of information-in-war and information warfare. Secondly, the Air Force has adopted terms unique to its service culture for internal use as it describes the concepts of IO. In effect, the terms are from an airman's point of view and facilitate his understanding of them, but the meanings are virtually the same as those used in the Joint lexicon. More importantly, this is instructive as it evidences the fact that the Air Force, like its sister services, is continuing along the path of doctrinal development for IO. Equally important, in doing so many in the Air Force are continuing down the path and are actively involved in this debate.

From an Army perspective, it may be key to note that the Air Force has a clear vision that information operations can be, are and will be, conducted in a global environment akin to air and space operations. The Air Force believes that because of its experience in these global environments that it is uniquely suited to conduct information operations throughout the global information environment, across the continuum from peace through high intensity conflict and throughout the breadth and depth of the battlespace in all four domains.[40]

It appears clear that, prompted by TS3600.1 and CJCS MOP 30, the Air Force followed suit, entered the debate and began the process of doctrine development. Like the Army, the path to IO doctrine for the Air force has not been easy or smooth, but it continues unabated and perhaps even stronger today than when it was first initiated.

US Navy Information Operations

The development of IO in the Navy is similar to that of the Army and Air Force. It begins after DESERT STORM in response to DODD TS3600.1 and CJCS MOP 30. In April 1994 the Navy issued its policy on Information Warfare/Command and Control Warfare in OPNAVINST

3430.25. In this Instruction the Navy directed that IW be implemented throughout the Naval service, it also identified and assigned key IW responsibilities within the Navy.

In August 1994 the Navy established the Naval Information Warfare Activity (NIWA). As a Department of the Navy activity, NIWA has numerous key IW responsibilities, to include: acting as the Navy's interface to sister service and national level agencies regarding information warfare technologies and acting as principal technical interface with the Fleet Information Warfare Command (FIWC). Unique in the Navy's acquisition process, NIWA has responsibility for generating IW requirements and for the procurement of IW systems.[41]

The Chief of Naval Operations (CNO) released Implementing Instruction For Information Warfare/Command And Control Warfare (IW/C2W), OPNAVINST 3430.26, in January 1995. This document defines IW as "action taken in support of national security strategy to seize and maintain decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence while protecting friendly information systems." In it, C2W is clearly a subset of IW conducted by the military to cause the practical effects of IW on an adversary. OPNAVINST 3430.26 also identified and assigned key IW/C2W responsibilities within the Navy. [42]

Only a few months later, in May 1995 the Navy published Naval Doctrinal Publication 6 (NDP 6), Naval Command and Control, as one of its six fundamental (the Army would call it a "capstone") doctrinal publications. Of relevance to this paper, NDP 6 takes note of the information revolution, acknowledges both the offensive and defensive applications of IW, and reiterates that C2W is a subset of IW. Although NDP 6 notes that information used to influence an adversary can be a powerful weapon, much more emphasis is placed on information for its use in decision-making.[43]

In 2000, Information Operations for the U.S. Navy: Control of the Information Battlespace for Maritime Dominance, a White Paper, was published. It quotes Joint Pub 3-13 for the definition of information operations and uses a diagram reminiscent of the diagrams in JV 2010 and JV 2020 in its section on IO and maritime dominance.[44] This White Paper introduces a new term, knowledge superiority, to the IO vocabulary. Although the words used to define knowledge superiority differ significantly from those used by the Joint Staff and the Army to define information superiority, in its meaning knowledge superiority is very similar to information superiority. This White Paper acknowledges that IO is a relatively new concept whose Joint doctrine was published in 1998. It addresses a concept for IO, defines maritime IO, considers the application of IO from the strategic to tactical level, suggests an organization for Navy IO and offers some thoughts on operationalizing IO. In this White Paper IO is viewed as a vital

contributor to knowledge superiority. It is seen as the power projection and force protection application of information technologies in information operations and as an enabling function, much the same as it is in the Joint and Army doctrine.[45]

For the Navy, like the Army and Air Force, the development of IO (and IW and C2W) has been an evolutionary process. Instigated by the OSD and JS policies and doctrine, educated by the writings of sister services and others (in and out of the military), and influenced by its own culture, the Navy has traveled a path similar to those of her sister services. This path involved changing IO terms, definitions and concepts; assigning and reassigning IO responsibilities; and, organizing or reorganizing for IO, over time. This trend can be expected to continue for some time to come.

ARMY INFORMATION OPERATIONS CHALLENGES

The preceding review of the Army's response to emerging IO concepts, DoD policy, and Joint Doctrine, and the responses from the sister services, demonstrate some shared areas of difficulty regarding IO doctrine, organizations, and technology. These difficulties represent significant challenges to the full realization of JV 2020. An in-depth treatment of the inherent complexity of all of these issues is beyond the scope of this paper. However, since the Army is particularly sensitive to the organizational implications of IO – in regard to doctrine (to include staff relationships) and training – specific attention will be given to these areas.

INFORMATION OPERATIONS DOCTRINE

There are three aspects of the doctrine problem of IO that need to be addressed: (1) the remaining ambiguity and confusion of the terminology, (2) the problem of IO weapons, and (3) the roles and functions of IO specialists in Army fighting units. These aspects will be considered in sequence.

Lingering Problems with Terms

The first doctrinal problem is the confusion caused by the many and rapidly changing concepts and definitions of information operations and its associated terms. To make matters worse, the definitions of these terms and the concepts they represent are not as well developed or as functional as they need to be to facilitate Army efforts to meet current and future challenges. The ODCSINT Information Operations Team summarized the problem as follows: "The concept of information operations means different things to different services and even branches within the services. The basic issue that has hampered the development of an effective Information Operations program in the Army is the lack of clearly defined doctrine."[46]

FM 3-13 does not strongly emphasize, or even adopt, a forward-looking IO concept that will lead the Army into and through Transformation. This draft doctrine does not recognize information as a domain unto itself, an attractive target and powerful weapon. It is far from hinting at any thoughts of IO as significant and common as the infantry, armor and aviation operations. It only addresses IO in the sense that IO is an enabler for other operations. It is true and good as far as it goes; the challenge is that it does not go far enough. Information operations can be the military means of choice as either the principal or sole way to achieve an end.

Doctrinal ambiguity has been compounded by the rapid evolution of the technology and the vocal debate about the ability of the services to transform in keeping with the postulated "revolution in military affairs." This rapid (r)evolution has manifested itself with the publication of at least three OSD, two Joint Staff and two Army documents in the past eight years which address the subject. This is actually the "double-edged sword" problem. On one edge, as noted above, doctrine is changing so fast that the lag time between conceptualization and publication can lead to confusion and misunderstanding, while simultaneously making it extremely difficult to stay current. On the other edge, the larger environment, especially the state of the art of technology, is changing so fast that doctrine (even as fast as it is changing) cannot keep pace. The Army's challenge here is to significantly reduce the lag time for the development and publication of doctrine. In some ways this challenge is analogous to that of material acquisition. The realities of the environment in which the Army operates are rapidly and continuously changing. These realities are evident in the ever-unsettled international situation; dynamic domestic politics; revolutionary advances in technology; and, frequent revisions to national security strategy, defense policy and joint doctrine.

> War and conflict have many constants. They always embrace wills, skills and kills. Command and control always has to deal with uncertainty and has to overcome the inevitable friction, "this terrible friction" as we learned from Von Clausewitz. Finally, there is always change and surprise to deal with. The essence of command is, to succeed in spite of all odds. New, however, might be the mastery to wage war in a new dimension, like on land at or below sea level, in the air or in space. It is precisely the growing understanding that there is something like a "cyberspace" or "information sphere" that makes information operations a real concern. The challenge is here and now.[47]

Weaponization

The second doctrinal problem is a reluctance to acknowledge or appropriately address the fact that some elements of information operations could actually be employed as weapons. This follows from the problem addressed above and will inevitably lead to significant problems in

the planning, training, advisability, and execution of such information operations. The FM 3-13 does not fully and explicitly identify all the elements of information operations that have the near term potential, or current, capability to be used as a weapon. Although, one must concede that the manual does address physical destruction, an element of information operations that clearly implies the employment of weapons as we have traditionally known them. As a result, doctrine does not provide guidance or procedures for the planning, coordination and execution of operations employing "weaponized" information operations capabilities. This will leave a generation of soldiers and leaders unaware of such weapons and ill prepared to use them. Information operations are an increasingly significant tool of war. In many cases certain information operations are the actual application of "weapons" against an adversary. As such, these specific information operations are becoming and will in the near future become as important (potentially more important) a weapons system in the Army inventory as rifles, tanks, artillery, and attack helicopters.

This invites the questions, if there are IO weapons, who pulls the trigger; or, who yanks the lanyard? By way of a leading analogy another question, when did Army aviation become a combat arms branch? The relevance of these questions to this paper is the significant concern that the doctrine being developed does not consider or integrate these concepts; and that this doctrine does not lead the Army into the future. As one brilliant Army officer has said, IO can become the "non-kinetic arm of decision in the future."[48] However, this can only be accomplished if these concepts are well understood and properly captured in doctrine.

Staff Organization and Responsibilities

The third doctrinal problem is the issue of staff proponency for information operations. This is the question of where in the organizational structure will the information operations function reside? Once determined, this will define where the information operations personnel will be assigned. Additionally, FM 3-13 does not address the information operations section at brigade and battalion. In the current state of doctrinal development, this question has not yet been finally resolved or approved.

The Information Operations field manual of 1996 did not assign the responsibility for information operations to any one specific staff officer. It leaves it up to the operations officer, G3, to manage information operations through one of his subordinates; the default position is a subordinate officer within the G3 section. As noted earlier, FM 3-13 was in development for some time. Among others, one reason for this was the fact that the various stakeholders

(Intelligence and Signal Centers, DCSINT, DISC4, and DCSOPS) could not agree on the staff organization for information operations.

> Early editions of TRADOC's FM 3-13 designated the G-6 as the information operations lead and combined Information Operations and Information Management (IM) functions and responsibilities under the Information Operations Officer's control. This proposal was strongly opposed by the DCSINT, DCSOPS and others.[49]

Finally, this issue begs the question of who on the staff should be responsible for information superiority. The default position in FM 3-13 gives this responsibility to the Chief of Staff and gives him the option of delegating it to one of his coordinating staff officers. The doctrine does not specifically give the responsibility for information superiority to any specific staff officer. This is a disconcerting omission, as it does not doctrinally cause someone to focus on IS. By default, the Chief of Staff is relegated to being the Information Superiority Officer by virtue of coordinating the efforts of the G2 (responsible for Intelligence), G3 (responsible for Surveillance and Reconnaissance), G6 (responsible for Information Management) and the G7 (IOCOORD). However, FM 3-13 does take this into account. As could be expected, the Chief is authorized to designate one of the coordinating staff officers as his agent to achieve information superiority by synchronizing IO, IM and ISR. As experience in countless tactical operations centers will attest, the responsibilities for information superiority will most likely be delegated to the G3.

TRAINING AND PROFESSIONAL DEVELOPMENT OF IO OFFICERS

The Army is banking on the ability of officers who are trained in Functional Area (FA) 30 to pull together all the different strands of concepts and capabilities that represent IO and fashion them into an effective tool for warfighting commanders. "Properly coordinating and utilizing these assets is a monumental responsibility that should not be underestimated."[50] This expectation may be very ambitious because the actual ability to train these officers and soldiers is in a state of near crisis. For example, a review of the Joint Information Operations Planning Handbook indicates the magnitude and complexity of the role of the information operations officer. The number of capabilities he must be cognizant of, and conversant in, as well as the number of staff principals and other subject matter experts he must coordinate with is staggering. And, the Army does not have a training course in place or programmed to properly prepare information operations officers for this responsibility. Clearly the challenge is training.

The problem is inadequate training and preparation of FA 30, Information Operations Officers, prior to their assignment to the field. FM 100-6 does not address the training

requirements or prerequisites for personnel conducting the information operations functions. Its successor, final draft FM 3-13, does not address the training requirements or prerequisites for Information Operations Coordinators. The overwhelming number of FA 30 officers enter the information operations career field with very little or no background, experience or training in the field of information operations. These are the officers, Major through Colonel, who will be assigned to Joint and Army billets as the information operations officer.

Currently, training for information operations officers is much too limited to permit them to be successful. This problem is compounded for the officers and the Army, as the recent and soon to be accessed FA 30s are assigned to their units. To be able to build rapport and credibility with their fellow staff officers and subordinate unit commanders and to gain the trust and confidence of their commanders, information operations officers must not only be tactically and technically competent, they must be the information operations subject matter expert. This newly assigned IO officer must be trained well enough to truly qualify him to coordinate the efforts of all the elements of IO on behalf of the commander. Regardless of the echelon of command (brigade, division, corps or above) at which the new information operations officers enter the field they must have the training to permit them to execute their duties in a professional and successful manner. The current state of information operations in the tactical and operational Army, as well as the future of Army information operations, is dependent upon the success of this first cohort of information operations officers assigned to tactical and operational Army command(er)s. These newly assigned information operations officers must perform at least as well as their counterparts on the coordinating and special staff to earn the respect, trust and confidence necessary for them, their successors and the FA-30 career field to survive.

A significant potential result of a lack of success by this first group of FA-30 officers is the demise of the FA-30 career field. Poor performance by this first cohort of FA-30 officers could cause our current tactical and operational commanders and their staffs to lose faith in information operations officers and in information operations. As result, the FA-30 officers may well receive unsatisfactory performance reports, thereby diminishing their potential for promotion. Observation of their performance by other officers coupled with knowledge of less than satisfactory reports would serve as a tremendous disincentive to other officers who otherwise may have considered FA-30 career field designation.

One obvious problem with training is a lack of funding. There is no lack of understanding, competence or focus on the part of those currently developing and implementing training for FA 30 officers. It is not within the scope of this paper to argue programmatics. However, the

significance is that the proper and necessary training must be developed and conducted for the IO officer and the FA 30 career field to survive. The loss of, or inability to develop, these officers will spell failure for the future application and development of IO in the Army. If that occurs, the Army will likely not be able to provide information superiority for itself and will not be able to conduct information operations in support of the joint force commander.

The current construct for FA-30 training is an extremely short four weeks consisting in equal parts of computer based training and classroom training.[51] By way of comparison, the following is offered for consideration: Functional Area 24, Telecommunications Systems Engineer, training is 20 weeks[52] long and FA 34, Strategic Intelligence Officer, training is 18 months long to include a masters degree.[53] One cannot imagine let alone truly believe that this limited training will prepare recently accessed FA-30 Officers with very little to no information operations experience or training to be successful as the commander's principal information operations advisor. Information operations officers must coordinate and plan for all the various elements and related activities of information operations and must be equally competent to his peers on the staff. Four weeks of training is inadequate. The information operations officer leaving this training for the field will, almost certainly, not have a competent information operations staff section chief to serve as his mentor and trainer. Neither will he have an extremely knowledgeable and experienced information operations counterpart at the next higher level of command as none have yet been formally trained and only very few have real world experience. [54]

This section identified challenges faced by the Army in the field of information operations. It identified three challenges in the area of IO doctrine and it identified the challenge of inadequate training and preparation of IO Officers. The following section of the paper will provide recommendations to redress these challenges.

RECOMMENDATIONS TO ADDRESS THE CHALLENGES

> Refinement of doctrine and the arrival of school trained FA 30s at units will enable the Army to operationalize Information Operations.[55]

INFORMATION OPERATIONS DOCTRINE

The three doctrinal challenges that the Army must meet are ambiguity and confusion in IO concepts and terminology (coupled with the lag time to publication), the issue of IO weaponization; and, the question of IO roles and functions.

Terms and Concepts

The Army must expand upon and clarify the concepts of information operations to ensure functionality and provide a view to the future. The clarification and expansion of IO concepts would include a treatment of information as a domain unto itself; information as an attractive target; and, information as a powerful weapon. The Army must fully integrate the concept of offensive IO, to include computer network attack. The Army must accept, and use to its advantage these concepts; it should further develop and then integrate them into doctrine. This will increase exposure to the concepts across the force and facilitate learning and understanding. As soldiers and leaders gain experience with IO, they will provide sound recommendations for more improvements to doctrine and TTP.

The definition of information operations found in the current final draft of FM 3-13 are acceptable, it provides the conceptual underpinning to allow the Army to fully support requirements implied by JV 2020. Obviously, this enabling function is valid, appropriate and useful. However, it is vital, that the Army not confine itself in its approach as it can limit thinking and prevent full consideration of all aspects of information operations. The Army must see IO as more than enabling functions. The Army must determine how to exploit information as a domain, target and weapon and codify it in the appropriate doctrine. The Army must conceptualize IO as a non-kinetic combat arm of decision, and IO operations as a principal means to mission accomplishment, somewhat akin to fire and maneuver, and fires. The Army must fully consider the offensive use of IO and develop the doctrine now that integrates IO much the same way that infantry, armor and attack aviation operations are integrated. The offensive use of the twelve elements of IO, as offensive is used in FM 3-13, to include those elements of information operations with which the Army is comfortable, such as physical destruction and electronic warfare must be continued.

The rapid advance in information technology combined with the current lag time to publication and the challenge of maintaining current and relevant doctrine begs the question whether the Army should adopt a new approach to doctrine development and dissemination. The answer is yes! The Army needs to develop and field a high technology, state of the art system, for doctrine development and dissemination. This system should be a completely digital, collaborative, electronic system for developing, staffing, approving, disseminating and updating doctrine. This system should permit updates and changes to doctrine as frequently as changes in the environment demand.

Weaponization

> Desert Storm provided a glimpse of things to come. Electronic microchips with a computer virus were reportedly inserted into a printer being smuggled into Iraq via Jordan for delivery to an air defense bunker. The virus was designed to disable the computers that enabled coordination and communications between air defense batteries. According to one account, it devoured "Windows" whenever technicians opened monitor screens to check on aspects of the air defense system.[56]

The challenge is the Army's reluctance to acknowledge or appropriately address elements of IO as weapons. Today, ten years after Desert Storm most reasonable military thinkers would agree that capabilities in addition to those suggested in the quote above exist. It is also likely that more are being developed today. Certainly in the very near future, these capabilities will be known and possibly used as weapons. The Army should clearly acknowledge this capability, or eventuality, and develop the doctrine that will allow soldiers and leaders to train, plan for and, when required, employ these weapons in the execution of information operations. Although FM 3-13 has taken a positive step to include a discussion of computer network attack and its viability in both offensive and defensive information operations, it does not go far enough. Army doctrine could begin to address IO weapons capabilities as it does other weapons systems.

One can envision the day, in the not to distant future, when commanders and decision makers at all levels will consider information as much a weapon as they do rifles, tanks, artillery and missiles. Given the acceptance of information as a domain, weapon and target, the Army's clarification in FM 3-13 needs to focus on the doctrinal applications and integration of information operations systems as weapons. Not only will the Army be operating in the information realm, but it will also be using information and information systems as weapons. The Army must prescribe the process for training, planning and executing operations with the information weapon. Prescribing these processes will not be easy, but the Army cannot wait for someone else to develop this competency first. It will take considerable effort, however, the Army does have a very talented and knowledgeable, albeit small, corps of information operations experts with which to accomplish this.

Staff Organization and Responsibilities

The Army should accept the developing construct for IO staff organization and responsibilities in the draft FM 3-13. This construct provides for professional information operations officers at ASCC, Corps and Division level. It creates the ACoS, G7, IO Coordinator position at Corps and Division, elevating the position of the IO officer to that of a principal on the coordinating staff at these echelons. This organizational construct provides the IO coordinator

higher visibility and, more importantly, greater access to the commander. This alignment maximizes the potential interaction between the commander and his IO expert while simultaneously minimizing the number of filters between the two. Operationally, it relieves the heavily burdened G3 of some responsibility and work and provides him a peer, competent as an IO staff officer, with whom to coordinate. It also provides for the health of the FA 30 career field, as it will result in increasingly responsible duty positions (at the various echelons) and viable career progression. Next, to the question of who is responsible for information superiority? It remains a viable course of action to leave it as is in FM 3-13, undefined. This then defaults to the Chief of Staff.

TRAINING AND PROFESSIONAL DEVELOPMENT OF IO OFFICERS

The training program for FA 30 officers must be significantly more in-depth and robust than is currently planned. A minimum of six months of training is required, to include at least four months of classroom training and at least two months of on the job experience. Subject matter experts (SMEs) must work out the exact details of the training program, however, thoughts for a baseline-training program for FA 30 officers follow.

The FA 30 officer should receive a significant familiarity with each of the twelve elements and two related activities of information operations, perhaps as little as one week or as much as four weeks of study in each element and activity. This could probably be accomplished at Fort Leavenworth with SMEs on staff or with SMEs from the appropriate TRADOC centers and schools. The intent is not to make each FA 30 officer a SME in every element of IO, as that is virtually impossible. Rather, the concept is to significantly familiarize each FA 30 officer with all the elements and related activities of IO. This familiarization should provide a depth of knowledge to make these officers intelligently conversant in each of the elements. As envisioned, this training would be far short of that required to qualify an officer to serve as the principal staff officer or commander of a section or unit assigned the mission of that element.

Additionally, these officers will require a thorough understanding of the intelligence necessary to support information operations, a basic understanding of how and where to request intelligence support, and an understanding of the information they should provide as input to the intelligence system.

Upon completion of this classroom training and prior to assignment to a command the new FA-30 officer should receive on the job training at the USAINSCOM Land Information Warfare Activity (LIWA). This should consist of hands on training to familiarize the FA-30 with the roles, missions, functions, capabilities and processes of the LIWA. This prepares the FA 30

with a baseline of knowledge in the processes that he will be expected to perform when assigned to his unit, as well as an appreciation of the expertise and support available from the LIWA. Finally, the new FA-30 should get a "real world" information operations experience working with a LIWA team employed and/or deployed to provide information operations support to a combatant command, an Army Service Component Command (ASCC), or an ARFOR.[57]

At some point, perhaps after the first or second assignment to an information operations officer position, the FA-30 officer should receive advanced civil schooling or post graduate education which directly enhances his capabilities as a FA-30 officer.

CONCLUSIONS

The Army has a requirement to ensure that it can conduct information operations to provide information superiority for its forces and to contribute to the information superiority of the Joint Force Commander. To do less would be to minimize, or abdicate, the Army's role in this vital aspect of national security. Over the past ten years the Army, along with the OSD and the Joint Staff, has made significant progress in the area of information operations. Unfortunately, the Army's development of information operations has not kept pace with the rapidly changing environment in which the Army exists and must operate. The Army can and must do significantly better to ensure that it satisfies its requirements for the foreseeable future.

Army doctrine for information operations must be developed, approved and disseminated in short order. Thereafter, it must be continuously updated in a timely manner. This doctrine must address today's capabilities but must also be forward looking, functional and comprehensive. It must anticipate future information operations capabilities, predicated on the known and postulated advances in technology, and on expected future Army missions.

The "weaponization" of some elements of information operations has occurred. Inevitably, these capabilities will become more common and available. The Army must recognize this and prepare for it now.

The Army has recognized the need to specify the staff organization and responsibilities information operations. It must continue to do so. Equally important, the Army must improve the training provided to qualify officers in Functional Area 30.

WORD COUNT=13,074

ENDNOTES

[1] John Schwartz, "When Point and Shoot Becomes Point and Click," The New York Times (12 November 2000): 4.16 [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI article reference no. NYT-3693-280.

[2] U.S. Joint Chiefs of Staff, Unified Action Armed Forces (UNAAF), Joint Pub 0-2 (Washington, D.C.: U.S. Department of Defense, 24 February 1995): I-2. Joint Pub 0-2 describes national security strategy as "the art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, informational) to achieve objectives that contribute to national security."

[3] "Strategic Information Warfare," The Futurist 31, (September/October 1997): 15 [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 014597703392603.

[4] Henry H. Shelton, Joint Vision 2020 (Washington, D.C.: U.S. Government Printing Office, 2000).

[5] Brenda P. Rivers, "Information Warfare: Where's the Action?," Journal of Electronic Defense 23 (October 2000): 53 [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI article re. no. FJEL-49-33. Ms. Rivers was quoting MAJ Barry Venable.

[6] Samuel B. Griffin, ed., Sun Tzu: The Art of War (London: Oxford University Press, 1971), 66-67.

[7] Brian K. Fredericks, "Information Warfare at the Crossroads," Joint Force Quarterly 16 (Summer 1997): 97. The general theme of this paragraph was gleaned from this reference.

[8] U.S. Joint Chiefs of Staff, "Command and Control Warfare, Memorandum of Policy No. 30", 8 March 1993; available from <http://www.eucom.smil.mil/eccs-or/library/Publications/MOP/GO30.ASC>; Internet; accessed 26 February 2001.

[9] Dan Kuehl, "Defining Information Warfare," The Officer 73, (November 1997): 31 [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI Publication no. 03552663. This article by Dr. Kuehl, then a professor of Information Warfare at National Defense University, provided insights into MOP 30. He also wrote in this article that "One of the hallmarks of C2W is that it can be conducted in any of the warfighting environments, land, sea, air, outerspace, even cyberspace..."

[10] Les Aspin, Annual Report to the President and Congress (Washington, D.C.: U.S. Government Printing Office, January 1994), 244; quoted in Brian E. Fredericks, "Information Warfare at the Crossroads," Joint Force Quarterly 16 (Summer 1997): 98.

[11] Department of the Army, Information Operations, Field Manual 100-6 (Washington, D.C.: U.S. Department of the Army, 27 August 1996), 2-2. Field Manual 100-6 quotes the CJCSI 3210.01 definition of information warfare.

[12] Joint Chiefs of Staff, Joint Doctrine for Command and Control Warfare (C2W), Joint Pub 3-13.1 (Washington, D.C.: U.S. Department of Defense, 7 February 1996), v.

[13] Ibid., GL-8.

[14] John M. Shalikashvili, Joint Vision 2010 (Washington, D.C.: U.S. Government Printing Office, July 1996), 16.

[15] U.S. Joint Chiefs of Staff, Enabling the Joint Vision, (Washington, D.C.: U.S. Department of Defense, May 2000), 1. Although published in 2000, the quote is relevant and appropriate at this point in the paper as it refers to JV 2010.

[16] Fredericks, "Information Warfare at the Crossroads," 97.

[17] Shelton, 20.

[18] William S. Cohen, "Statement of the Secretary of Defense William S. Cohen in Connection with the FY 2001 Defense Budget Senate Armed Services Committee," 8 February 2000; available from <http://www.defenselink.mil/dodgc/lrs/docs/test00-02-08Cohen.htm>; Internet; accessed 27 September 2000.

[19] Department of the Army, Concept For Information Operations, TRADOC Pamphlet 525-69 (Fort Monroe, VA: U.S. Department of the Army, 1 August 1995).

[20] Ibid., i-2.

[21] Ibid., 4.

[22] Department of the Army, Information Operations, 2-2.

[23] Ibid., 2-3.

[24] Ibid., iii-v.

[25] Ibid., 6-7.

[26] Information Operations Team, ODCSINT, HQDA, The Way Ahead for Information Operations, White Paper, Working Papers (Washington, D.C.: U.S. Department of the Army), 3. This White Paper is a working paper and is not a final document approved by The DCSINT. The Information Operations Team uses it as a think piece and as a point of departure for discussion with others.

[27] Department of the Army, Information Operations, D-0 – D-1.

[28] Ibid., D-1.

[29] There also were several administrative issues that probably added time to the preparation of the final draft. These include the transfer of responsibility for information operations from headquarters TRADOC to the Combined Arms Doctrine Directorate, a debate as to whether to produce capstone doctrine or TTP, and, probably a few re-writes from scratch based upon reassignment of those in charge with their own views on the subject. In the end, this is probably as normal as it is abnormal in the development of doctrine in the Army.

Regardless of the reason(s), the inability or unwillingness of the Army to develop and publish information operations doctrine in a timelier manner has a potentially serious deleterious effect on the capability of the Army to conduct information operations.

[30] Department of the Army, "Information Operations: Doctrine; Tactics, Techniques and Procedures," Field Manual 3-13, Final Draft, 30 September 2000; available from <http://www.cgsc.army.mil/cdd>; Internet; accessed18 November 2000.

[31] Information Operations Team, ODCSINT, HQDA, White Paper, 3.

[32] Department of the Army, "Information Operations: Doctrine; Tactics, Techniques and Procedures."

[33] Ibid., 1-10 – 1-12. In specific the quote and in general the ideas in this paragraph are gleaned from this source.

[34] Ibid., F-1 – F-7.

[35] An observation, perhaps a significant issue, brought to light by this chronological review is the fact that our current process for doctrinal development and dissemination is much too cumbersome and slow. It will likely disadvantage the Army significantly if it is not corrected.

[36] Ronald Grahek <rong@erols.com>, "Greetings and Help, The Paper," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 4 March 2001; and, Steven D. Mabeus <sdmabeu@LIWA.belvoir.army.mil>, "Follow-Up to Phoncon, Request for Help," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 11 January 2001.

[37] Brian Fredericks, "Information Warfare: The Organizational Dimension;" available from <http://www.ndu.edu/inss/siws/ch4.html>; Internet; accessed 14 March 2001.

[38] Ronald R. Fogleman and Sheila E. Widnall, "Cornerstones of Information Warfare;" available from <http://www.af.mil:80/lib/corner.html>; Internet; accessed 16 December 2000.

[39] Department of the Air Force, "Information Operations," Air Force Doctrine Document (AFDD) 2-5, 1998; available from <http://hqafdc.maxwell.af.mil>; Internet; accessed 7 December 2000.

[40] Ibid., 37. This reference, AFDD 2-5 coupled with AFDD 2, provides this author a clear indication that the Air Force sees and/or seeks a special (overarching, DOD/Armed Forces-wide) role for itself in the IO field. AFDD 2 is a "capstone" doctrine document for the Air Force. (Organization and Employment of Aerospace Power, Air Force Doctrine Document (AFDD) 2 (Washington, D.C.: U.S. Department of the Air Force, 17 February 2000) 74-75.)

[41] The Fleet Information Warfare Command (FIWC) focuses on the Atlantic and Pacific Fleets serving as the link between them and the Naval Information Warfare Activity (NIWA). NIWA focuses longer term and to higher and adjacent levels of IW activity, while the FIWC focuses shorter term and down to the fleets.

[42] Department of the Navy, Implementing Instruction for Information Warfare/Command and Control Warfare, OPNAVINST 3430.26 (Washington, D.C.: U.S. Department of the Navy, 18 January 1995), 1. The remainder of the information in this paragraph is gleaned from throughout the cited reference. OPNAVINST is naval shorthand for Operations Naval Instruction.

[43] Department of the Navy, "Naval Command and Control," 19 May 1995; available from <http://www.nwdc.navy.mil/doctrine/docs/Ndp6/ndp60005.htm>; Internet; accessed 15 March 2001. Chapter three, "The Naval Command and Control System" addresses the role of information. Chapter four, "Building Effective Command and Control," addresses the information revolution.

[44] The diagrams in JV 2010 (page 26) and JV 2020 (page 2) are those that depict the four operational concepts executed in an environment of information superiority leading to full spectrum dominance.

[45] Department of the Navy, Information Operations for the U.S. Navy: Control of the Information Battlespace for Maritime Dominance, A White Paper (Washington, D.C.: U.S. Department of the Navy, 8 September 2000).

[46] Information Operations Team, ODCSINT, HQDA, White Paper, Working Papers, 5.

[47] J. M. J. Bosch, "Information Operations – Challenge or Frustration?," Military Technology 24 (May 2000): [database on-line]; available from UMI ProQuest Direct, Bell & Howell, UMI article reference no. FMTC-33-30.

[48] Russell C. Rochte <rochter@leavenworth.army.mil>, "Comments to draft," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 6 March 2001.

[49] Information Operations Team, ODCSINT, HQDA, White Paper, 5.

[50] Information Warfare Division, Joint command and Control Warfare School, Armed Forces Staff College, "Joint Information Operations Planning Handbook." Preliminary Draft. Available from <http://www.jwfc.js.mil>; Internet; accessed 22 February 2001. Other ideas regarding the enormity of the tasks facing the IO Officer are also addressed in this source. Although this handbook addresses the joint environment, it is conceptually the same for the Army.

[51] U.S. Army Command and General Staff College, "Functional Area 30, Information Operations," 22 January 2001; available from <http://www-cgsc.army.mil/dao/fa30>; Internet; accessed 7 March 2001.

[52] U.S. Army Signal School and Fort Gordon, "Telecom systems Engineer Course"; available from <http://www.gordon.mil/fa24/default.htm>; Internet; accessed 15 March 2001.

[53] U.S. Army Intelligence Center and Fort Huachuca, "FA 34, Strategic Intelligence Officer," 26 January 2001; available from <http://huachuca-usaic.army.mil/ocmi/officer.html>; Internet; accessed 15 March 2001.

[54] Steven D. Mabeus <sdmabeu@LIWA.belvoir.army.mil>, "Follow-Up to Phoncon, Request for Help," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 11 January 2001, and, Russell C. Rochte <rochter@leavenworth.army.mil>, "Comments to draft," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 6 March 2001.

[55] Information Operations Team, ODCSINT, HQDA, White Paper, Working Papers, 7.

[56] Dennis B. Herbert, "Non-Lethal Weaponry: From Tactical to Strategic Applications," Joint Force Quarterly 21 (Spring 1999): 89.

[57] Steven D. Mabeus <sdmabeu@LIWA.belvoir.army.mil>, "Follow-Up to Phoncon, Request for Help," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 11 January 2001, and, Russell C. Rochte <rochter@leavenworth.army.mil>, "Comments to draft," electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>, 6 March 2001.

BIBLIOGRAPHY

Ackerman, Robert K. "Navy Doctrine, Systems Face Information Warfare Makeover." Signal 50 (July 1996): 19-21.

Air Land Sea Application Center. "Information Warfare/Information Operations Study." 15 December 1995. Available from <http://www.dtic.mil/alsa/pubs/iwio.pdf>. Internet. Accessed 14 March 2001.

Alberts, David S., and Daniel S. Papp, eds. The Information Age: An Anthology on Its Impacts and Consequences. Washington, D.C.: National Defense University Press, June 1997.

Aspin, Les. Annual Report to the President and Congress. Washington, D.C.: U.S. Government Printing Office, January 1994, 244. Quoted in Brian E. Fredericks. "Information Warfare at the Crossroads." Joint Force Quarterly 16 (Summer 1997): 97-103.

Baier, Frederick L. Intense Complexities: Some Conceptual and Practical Thoughts on Information, the Battlespace, and Organizing for Information Operations. A research project for the Institute for National Securities Studies. Maxwell Air Force Base, AL: U.S. Air Force Doctrine Center, September 1999.

Bosch, J. M. J. "Information Operations – Challenge or Frustration?" Military Technology (May 2000): 86-89. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI article reference no. FMTC-33-30.

Brand, Gary. Protecting the United States Against Information Warfare. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 1 April 2000.

Busby, Daniel J. Peacetime Use Of Computer Network Attack. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 3 April 2000.

Cardinal, Charles N. "Delivering Joint Information Superiority." Joint Force Quarterly 23 (Autumn/Winter 1999-2000): 47-50.

Center For Strategic and International Studies, Cybercrime ...Cyberterrorism ...Cyberwarfare ...Averting An Electronic Waterloo. Washington, D.C.: The CSIS Press, 1998.

Clinton, William J. A National Security Strategy For A New Century. Washington, D.C.: The White House, December 1999.

_____. The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. White Paper. Washington D.C.: The White House, 22 May 1998.

Cohen, William S. Report of the Quadrennial Defense Review. Washington, D.C.: U.S. Department of Defense, May 1997.

_____. "Statement of the Secretary of Defense William S. Cohen In Connection with the FY2001 Defense Budget." 8 February 2000. Available from

<http://www.defenselink.mil/dodgc/lrs/docs/test00-02-08Cohen.htm>. Internet. Accessed 27 September 2000.

Cunningham, Kevin R. Bounded Rationality and Complex Coupling: Challenges for Intelligence Support to Information Warfare. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 10 April 2000.

Eassa, Charles. "Information Operations News." 7 June 2000. Available from <http://www-cgsc.army.mil/dao/fa30/IO%20Reading%20File.htm>. Internet. Accessed 13 January 2001.

Fogleman, Ronald R., and Sheila E. Widnall. "Cornerstones of Information Warfare." Available from <http://www.af.mil:80/lib/corner.html>. Internet. Accessed 16 December 2000.

Fredericks, Brian E. "Information Warfare at the Crossroads." Joint Force Quarterly 16 (Summer 1997): 97-103.

_____. Information Warfare: The Organizational Dimension. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 7 February 1996.

Gompert, David C., and Irving Lachow. Transforming U.S. Forces: Lessons from the Wider Revolution. Issue Paper no. 193. Santa Monica, CA.: RAND National Defense Research Institute, 2000.

Grahek, Ronald <rong@erols.com>. "Greetings and Help, The Paper." Electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>. 4 March 2001.

Greenberg, Lawrence T., Seymour E. Goodman, and Kevin J. Soo Hoo. Information Warfare and International Law. Washington, D.C.: National Defense University, 1998.

Griffin, Samuel B., ed. Sun Tzu: The Art of War. London: Oxford University Press, 1971.

Herbert, Dennis B. "Non-Lethal Weaponry: From Tactical to Strategic Applications." Joint Force Quarterly 21 (Spring 1999): 87-91.

Horne, Jeffrey C. Information Superiority as an American Center of Gravity: Concepts for Change in the 21st Century. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 10 April 2000.

Information Operations Team, ODCSINT, HQDA. The Way Ahead for Information Operations. White Paper, Working Papers. Washington, D.C.: U.S. Department of the Army. This White Paper is a working paper and is not a final document approved by The DCSINT. The Information Operations Team uses it as a think piece and as a point of departure for discussion with others.

Information Warfare Division, Joint command and Control Warfare School, Armed Forces Staff College. "Joint Information Operations Planning Handbook." Preliminary Draft. Available from <http://www.jwfc.js.mil>. Internet. Accessed 22 February 2001.

Khalilzad, Zalmay M., and John P. White, eds. The Changing Role of Information in Warfare. Santa Monica, CA.: RAND, 1999.

Kuehl, Dan. "Defining Information Warfare." The Officer 73 (November 1997): 31-33. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI Publication no. 03552663.

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

Mabeus, Steven D. <sdmabeu@LIWA.belvoir.army.mil>. "Follow-Up to Phoncon, Request for Help." Electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>. 11 January 2001.

Mahnken, Thomas G. "War in the Information Age." Joint Force Quarterly 10 (Winter 1995-96): 39-43.

Miller, Russell F. Developing And Retaining Information Warriors: An Imperative To Achieve Information Superiority. Strategy Research Project. Carlisle Barracks, PA: U.S. Army War College, 29 February 2000.

Molander, Roger C., Peter A. Wilson, David A Mussington, and Richard F. Mesic. Strategic Information Warfare Rising. Santa Monica, CA: RAND, 1998.

National Defense Panel. Transforming Defense, National Security in the 21st Century. Arlington, VA.: National Defense Panel, December 1997.

Owens, William A. "The American Revolution in Military Affairs." Joint Force Quarterly 10 (Winter 1995-96): 37-38.

Reimer, Dennis J. Army Vision 2010. Washington, D.C.: Department of the Army, 1996.

Rivers, Brenda P. "Information Warfare: Where's the Action?" Journal of Electronic Defense 23 (October 2000): 53-56. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI article reference no. FJEL-49-33.

Rochte, Russell C. <rochter@leavenworth.army.mil>. "Comments to draft." Electronic mail message to Charles M. Borg <charles.borg@carlisle.army.mil>. 6 March 2001.

Rowe, Wayne J. Information Warfare: A Primer for Navy Personnel. Strategic Research Department Research Report 6-95. Newport, RI: U.S. Naval War College, 23 June 1995.

Schneider, James J. "Black Lights: Chaos, Complexity, and the Promise of Information Warfare." Joint Force Quarterly 15 (Spring 1997): 21-28.

Schwartz, John. "When Point and Shoot Becomes Point and Click." The New York Times (12 November 2000): 4.16. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI article reference no. NYT-3693-280.

Science Applications International Corporation. "Information Operations." 1998. Available from <http://sac.saic.com/io/io_content.htm>. Internet. Accessed 23 December 2000.

_____. Warfare Legal, Regulatory, Policy and Organizational Considerations for Assurance. Washington, D.C.: Telecommunications and Networking Systems Operation, 4 July 1995.

Shalikashvili, John. Joint Vision 2010. Washington, D.C.: U.S. Joint Chiefs of Staff, 1996.

Shelton, Henry H. Joint Vision 2020. Washington D.C.: U.S. Government Printing Office, 2000.

Sizer, Richard A. "Land Information Warfare Activity: IO and IW Support to Army XXI." Military Intelligence 23 (January-March 1997): 23-24.

Slavin, Jim. Close Access Information Operations. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 10 April 2000.

"Strategic Information Warfare." The Futurist 31 (September/October 1997): 15. Database on-line. Available from UMI ProQuest Direct, Bell & Howell, UMI publication no. 014597703392603.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters 1 (Spring 2000): 13-29.

United States Commission On National Security/21st Century. New World Coming: American Security In The 21st Century. Arlington, VA: United States Commission On National Security/21st Century, 15 September 1999.

_____. Seeking A National Strategy: A Concert For Preserving Security And Promoting Freedom. Arlington, VA: United States Commission On National Security/21st Century, 15 April 2000.

U.S. Army Command and General Staff College. "Functional Area 30, Information Operations." 22 January 2001. Available from <http://www-cgsc.army.mil/dao/fa30>. Internet. Accessed 7 March 2001.

U.S. Army Intelligence Center and Fort Huachuca. "FA 34, Strategic Intelligence Officer." 26 January 2001. Available from <http://huachuca-usaic.army.mil/ocmi/officer.html>. Internet. Accessed 15 March 2001.

U.S. Army Signal School and Fort Gordon. "Telecom Systems Engineer Course." 14 March 2001. Available from <http://www.gordon.mil/fa24/default.htm>. Internet. Accessed 15 March 2001.

U.S. Army War College. Information Operations Primer. Carlisle Barracks, PA.: U.S. Army War College, January 2001.

U.S. Department of the Air Force. "Organization and Employment of Aerospace Power." Air Force Doctrine Document 2. 17 February 2000. Available from <http://hqafdc.maxwell.af.mil>. Internet. Accessed 11 March 2001.

_____. "Air Force 2025." 12 November 1996. Available from <http://www.au.af.mil/au/2025quicklk.htm>. Internet. Accessed 11 March 2001.

_____. "Information Operations." Air Force Doctrine Document (AFDD) 2-5. 5 August 1998. Available from <http://hqafdc.maxwell.af.mil>. Internet. Accessed 7 December 2000.

U.S. Department of the Army. Command & Control Countermeasures (C2CM). Army Regulation 525-20. Washington, D.C.: 13 July 1992.

_____. Concept For Information Operations. TRADOC Pamphlet 525-69. Fort Monroe, VA.: U.S. Department of the Army, 1 August 1995.

_____. "Information Operations: Doctrine: Tactics, Techniques and Procedures." Field Manual 3-13. Final Draft. 30 September 2000. Available from <http://www.cgsc.army.mil/cdd>. Internet. Accessed 18 November 2000.

_____. Information Operations. Field Manual 100-6. Washington, D.C.: U.S. Department of the Army, 27 August 1996.

U.S. Department of Defense. Information Operations. Department of Defense Directive S-3600.1. Washington, D.C.: U.S. Department of Defense, 9 December 1996.

_____. Information Superiority: Making the Joint Vision Happen. Washington, D.C.: U.S. Department of Defense, 2000.

U.S. Joint Chiefs of Staff. Concept for Future Joint Operations, Expanding Joint Vision 2010. Washington D.C.: U.S. Department of Defense, May 1997.

_____. Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. Washington D.C.: U.S. Department of Defense, 10 June 1998.

_____. Enabling the Joint Vision. Washington, D.C.: U.S. Department of Defense, May 2000.

_____. "Command and Control Warfare, Memorandum of Policy No. 30". 8 March 1993. Available from <http://www.eucom.smil.mil/eccs-or/library/Publications/MOP/GO30.ASC>. Internet. Accessed 26 February 2001.

_____. National Military Strategy of the United States of America. Washington D.C.: U.S. Department of Defense, September 1997.

_____. Joint Doctrine for Information Operations. Joint Publication 3-13. Washington D.C.: U.S. Department of Defense, 9 October 1998.

_____. Joint Doctrine for Command and Control Warfare (C2W). Joint Publication 3-13.1. Washington D.C.: U.S. Department of Defense, 7 February 1996.

_____. Unified Action Armed Forces. Joint Publication0-2. Washington, D.C.: U.S. Department of Defense, 24 February 1995.

U.S. Department of the Navy. Implementing Instruction for Information Warfare/Command and Control Warfare. OPNAVINST 3430.26. Washington, D.C.: U.S. Department of the Navy, 18 January 1995.

_____. Information Operations for the U.S. Navy: Control of the Information Battlespace for Maritime Dominance. A White Paper, DRAFT8. Washington, D.C.: U.S. Department of the Navy, 8 September 2000.

_____. "Naval Command and Control." 19 May 1995. Available from <http://www.nwdc.navy.mil/doctrine/docs/Ndp6/ndp60005.htm>. Internet. Accessed 15 March 2001.

Whitehead, YuLin. "Information as a Weapon: Reality Versus Promises." Airpower Journal 11 (Fall 1997): 40-54. Database on-line. UMI ProQuest Direct, Bell & Howell, UMI publication no. 03514580.