US Armed Forces Information Operations- Is the Doctrine Adequate?

A Monograph
By
Major Charles N. Eassa
United States Army

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

First Term AY 99-00

Approved for Public Release; Distribution is Unlimited

20000315 065

DTIC QUALITY INSPECTED 3

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL

Major Charles N. Eassa

Title of Monograph: U.S. Armed Forces Information Operations - Is the Doctrine Adequate?

Approved by:

_____ Monograph Director
James Schnieder, Ph.D.

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

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

Accepted this xx Day of December 1999

ABSTRACT

US Armed Forces Information Operations:
Is the Doctrine Adequate? By MAJ Charles N. Eassa, USA, 46 pages.

The integration of Information Operations into the United States Armed Forces has touched every aspect and level of military operations. This paper seeks to answer whether joint and service Information Operations doctrine is adequate.

Ultimately, all military operations function on information. This requires an active thought process to protect the needed information and information systems as well as to exploit adversaries' information requirements. The sister services have pursued approaches in developing and resourcing Information Operations based upon their tactical requirements.

Outlining the joint and service doctrines, this monograph suggests that doctrine at the operational and strategic level is a collusion of service tactical doctrine and is too broad in its guidance. The doctrine does not specify responsibilities at the operational or strategic levels nor does it afford for synergy based on the services' Information Operations doctrine.

The study concludes that the doctrine represent a solid point of departure to continue the refinement and delineation of Information Operations at the operational and strategic levels.

Table of Contents

I. Introduction 5

II. Why is Information Valuable? 7

III. Current State of Information Operations Doctrine 9

Joint 10

USAF 12

USN 13

USMC 14

SOCOM 16

USA 16

IV. Systems Approach 19

V. Analysis 22

Relevancy 23

Jointness 26

Integration 28

Sustainability 30

Applying the Systems Approach 31

VI. Conclusion 32

I. Introduction

The predominate problem of the US Military is to compel and deter those who would oppose the will of the US and if unsuccessful, render them incapable of physical resistance.[1]

The Gulf War has been heralded by some as the first information-age war and by others as the last vestige of the Cold War. Regardless, the demise of the Warsaw Pact, the dawn of globalization and the explosion of technology in the 1990's have created new challenges, vulnerabilities and tools for the art of war.[2]

Since the close of the Cold War Era, the explosion and shock of technology have had an unprecedented impact. This impact is felt throughout the world as advances in communications and computers radically alter how money is made, relationships are formed and maintained, data exchanged, events reported and the increased value of information. It has even impacted what our nation's vital interest are; for what goals the policy makers of the United States are willing to send United States soldiers, sailors, airmen and marines into harm's way and the methods the military employs to achieve its mission.[3]

Nowhere is the impact felt greater than in the United States Armed Forces and in particular, the United States

Army. In response to this phenomenon and the growing complexity of warfare, the United States Armed Forces coined the term Information Operations to gather the many different disciplines affected by the changing tide. The basic premise of Information Operations is to protect one's own information and information dependent processes while taking action to degrade, deny or disrupt the adversary from using information he requires or depends upon to his advantage.

Despite the impact of new technologies and reports stating the conduct of warfare has changed forever, the purpose of warfare remains the same as it did in Napoleon's time. Carl von Clausewitz's statement that war is an extension of politics and is waged to impose one's will upon the adversary still holds true.

The integration of Information Operations into the United States Armed Forces has touched every aspect and level of military operations. While the fundamental concept of Information Operations is not new to the United States Armed Forces, its application and mindset offers different approaches to the complex challenges of today and tomorrow.

This paper examines the joint and services' doctrinal approach to information operations. It seeks to answer whether Information Operations doctrine is adequate at the

service component and joint level. Is the doctrine conceptual or practical? Does each service account for Information Operations across the spectrum of military operations and is it being resourced and applied? The paper uses relevancy, jointness, sustainability, and force integration as criteria.

II. Why is Information Valuable?

If each individual or group assigns its own value to information, how can a value be established? The answer lies in what the information is to accomplish. For the military, information intended to control forces or generate effects is critical. Information is the lifeblood of any command and control system.[4] Without the ability to coordinate, achieve or synchronize actions and effects, military power is subjected to degradation and is less than the sum of its parts. This is the foundation of command and control warfare.

Information is also critical to forming perceptions. Perception is defined as "the act or faculty of apprehending by means of the senses or of the mind; cognition; understanding".[5] Conveying information to build perceptions is a foundation to deterrence. The concept of

mutually assured destruction is an example of deterrence from the Cold War era.

Perception is a critical information element in support and stability operations as well. If a commander of a peacekeeping operation ensures that his adversaries understand exactly what his charter is and how he intends to accomplish it, the perception builds expectations. These expectations define the limits of what the adversaries may do before they violate the expected behavior.

Ultimately, all military operations function on information. Information is the source of the conflict or crisis. Information is what sets the military in motion to accomplish stated objectives. Information is how the military commands and controls its entities to accomplish these objectives. A specific aspect of information is what the military seeks to establish to achieve this endstate. The value of the information is equal to the expected outcome of achieving the desired end.

Understanding the value of information is critical for the United States Armed Forces for two reasons. The first is the ever-increasing dependency of United States Military on the free and uninterrupted flow of information. Ensuring the freedom to collect, analyze and pass

information and guidance is critical to any endeavor the military undertakes. This requires an active thought process to protect the needed information and information systems.[6]

The second reason is that the understanding of information and its flow can be a force multiplier. Given the global requirements and the reduced force structure, the military can use information to deter hostilities, increase doubt in an adversary's mind about chances of success, help to build world opinion against aggressors, and promote stability. Upon the initiation of conflict, the United States Military can affect the adversary's information to create opportunities to exploit and to degrade the adversary's ability to fight on his own terms.

III. Current State of Information Operations Doctrine

Conceptually, one conducts Information Operations to prevent adversaries from freely using information to achieve desired results while retaining the ability to use information and exploiting the adversary's information gap. Nation-states focus on imposing their will on other nation-states and non-governmental international players.[7] This is accomplished by applying all instruments of power available to the nation-state. The generally accepted categories are diplomatic, informational, military and economic (DIME). The dynamics of national instruments of power when viewed as a system have become increasingly interwoven and more complex. At the strategic level, the ability to control media sources is an excellent example.

Communist and totalitarian countries rely extensively on IO to retain power and place their experts at the highest government levels.[8]

Joint

In 1996, General John Shalikashvili, Chairman of the Joint Chiefs of Staff, signed Joint Vision 2010 to "provide an operationally based template for the evolution of the Armed Forces for a challenging and uncertain future".[9] The document is "front-end guidance for defense efforts to achieve future joint warfighting capabilities".[10] By applying dominant maneuver, precision engagement, full dimensional protection, and focused logistics, the United States will achieve full spectrum dominance. A key aspect of full spectrum dominance is the emerging importance of information superiority. It states that information superiority will mitigate the impact of the friction and fog of war, advocates ensuring an uninterrupted flow of information and advocates non-traditional actions.[11]

Joint Publication 3-13, Joint Doctrine for Information Operations, defines information operations as actions taken to affect adversary information and information systems while defending one's own[12]. Information Operations are targeted to affect information dependent processes, whether the processes are human or automated.[13] Information operations are split into offensive IO and defensive IO. Defensive IO is conducted continuously across the spectrum of peace, crisis and conflict. Offensive IO is information warfare by another name.

At the strategic level, the NCA directs the activities to achieve the national objectives. There is a great amount of cooperation at the interagency level. At the operational level, IO focus on affecting the adversary's lines of communication, his ability to command and control his resources and his ability to collect intelligence. However, the operational level is increasingly playing a critical role in the development and execution of the national policies in peacetime, crisis and war. Examples of this range from CINCs developing their theater engagement plan, reporting directly to congressional committees, and holding press conferences with coalition partners. Upon direction from the National Command Authority, the operational level is directed to affect the strategic level of another nation-state. The Gulf war and Kosovo are examples of this.

The publication states that the Chairman of the Joint Chiefs of Staff is responsible for establishing doctrine for integrating IO into joint warfighting. It charges the combatant commanders to develop their own processes to integrate all the capabilities associated with IO. The Chiefs of the Services and the Commander in Chief of United States Special Operations Command are charged to conduct research, development, testing and evaluation, and procurement of IO capabilities that meet validated service and joint requirements. They are further charged to organize forces with IO capabilities and to exercise IO across the range of military operations.

Each CINC is allowed to pursue independent avenues of IO. This fosters duplication of effort and complicates the shared lessons learned.[14]

Joint Publication 3-13 lays out the framework for information operations. It is split into offensive and defensive operations. "Offensive operations involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and or promote specific objectives".[15] Offensive Information Operation activities are operational security, military deception, psychological operations, electronic warfare, physical attack/destruction and special information operations. Special information operations are defined as "Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process".[16] They have the most effect and impact in peace and during the initial crisis stages. During combat operations, they are a critical force enabler.

"Defensive Information Operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect information and defend information systems. They are conducted through information assurance, operational security, physical security, counterdeception, counter-psychological operations, counterintelligence, electronic warfare, and special information operations".[17] Offensive Information Operations can support defensive Information Operations.

The joint community is actively pursuing avenues to organize and resource Information Operations. The Joint Command and Control Warfare Center, located at Kelly Air Force Base in San Antonio, has been renamed the Joint Information Operations Center and moved under SPACECOM for Computer Network

Defense (CND) and Computer Network Attack (CNA). It also has the mission to support each CINC with an Information Operations team.

To provide intelligence support and capabilities, the Joint Warfare Analysis Center has been stood up to review adversaries as a system. They provide detailed information on the infrastructure and how to affect it. The Information Operations Technical Center provides analysis on information systems, their capabilities and their vulnerabilities.

The number of agencies involved in Information Operations is growing. The Defense Information Systems Agency is charged with information assurance. The Joint Program Office for Special Technological Countermeasures stood up in 1997. The National Security Agency is heavily involved with the full spectrum of Information Operations. There is a great deal of interagency activity with the Departments of State, Treasury, and Justice.

USAF

Information Operations is a natural extension of Air Power. Both are centered on exploiting technology and achieving a degree of superiority to degrade or deny the adversary the freedom to react. Air Power has sought to cause adversarial leadership to capitulate by stripping away his ability to freely utilize his military, economic and national sources of power. To accomplish this, the Air Force must establish a certain degree of air superiority whether through stealth technology, targeting the integrated air defense system or attempting to cause shock by attacking the enemy throughout his depth simultaneously.

Likewise, Information Operations seeks to establish a degree of information superiority to ensure the adversary cannot effectively exploit his information to concentrate his resources. Without the proper information, an adversary cannot detect air attacks nor direct his fighter cover to the critical location in time and space. To achieve this end, the United States Air Force states in its capstone doctrine manual, Air Force Doctrine Document 1, that information superiority is one of its six core competencies.

Air power theorists essentially advocate the shock of Information Operations. Colonel John Warden's five ring theory focuses on the application of air power on critical targets to deny the adversary the ability to freely control his resources and to fight on the United States Air Forces' terms. Targeting adversarial

communication nodes during the Gulf War, Bosnia and Kosovo are clear indicators of the acceptance of Information Operations within the Air Force.

Air Force publications are filled with debate on how best to organize, apply and resource Information Operations. Within the Air Force, there are voices stating that Information Operations should be elevated to a unified command level. There are also views stressing the non-technological approach, "In addition to recklessly assuming inviolability of out reconnaissance and surveillance technology, this approach seriously underestimates the adversary's religious or revolutionary fervor".[18]

Currently, the Air Force is resourcing Information Operations throughout its structure. It is standing up Information Warfare wings aligned with numbered air forces. The Air Force Information Warfare Center, established in 1993, is co-located with the Air Intelligence Agency at Kelly Air Force Base, Texas. This enables the two agencies to work closely and develop mutually supporting doctrine and procedures for Information Operations.

Air Force Doctrine Document 2-5, Information Operations was published on 5 August 1998. A well written document, it lays out doctrinally how the Air Force should integrate Information Operations, who has responsibilities at what level and the relationship of Information Operations to all Air Force missions. In broad terms, it describes the desired effects of Information Operations at the strategic, operational and tactical levels of war.

Despite the title, AFDD 2-5 focuses only on information warfare. It does not address operations other than war. The general trend of the document is focused on the protection of Air Force information and denying the adversary his information during crisis and conflict.

USN

Naval warfare is centered on establishing control of sea-lanes. As sea lines of communication are vast, this involves a great deal of information to ensure resources are properly employed at the critical location and time. Modern naval warfare is extremely dependent upon centralized control of critical information to conduct its mission. By breaking the Japanese naval code during World War II identifying Midway as the

target for the next invasion, Admiral Nimitz was able to concentrate his outnumbered forces to foil the Japanese plan.

The United States Navy views information as the "lifeblood of any command and control system".[19] It is essential to ensure free flow of information to ensure effective command and control. To this end, the Navy places a great deal of priority on information protection. The Navy also recognizes this same vulnerability as an opportunity to exploit. It views information warfare as another tool for attacking adversaries and controlling sea lines of communication. Information Operations and Command and Control Warfare are almost synonymous in the eyes of the Navy.[20]

To this end, the Navy has established the Fleet Information Warfare Activity in 1995 to support Information Operations throughout the Navy organization. It has always maintained a strong command and control warfare organization and has readily converted these to Information Operations units.

As the Navy is technically oriented, it expends a great deal of effort to research and resource information warfare. This is reflected in Admiral Owen's phrase "system of systems". It reflects the Navy view that its (and the nation's) adversaries are systems. As information is the blood pulsing through the system's veins, disrupting, denying or degrading the blood flow will cause the system to cease functioning properly.

This is manifested in the lack of written Navy Information Operations doctrine. While a firm believer in Information Operations, most of the Navy's written information resides in technical documents, posits, directives and classified sources. While most naval officers can describe their role in information operations, they cannot cite doctrinal references.

USMC

The United States Marine Corps published "A Concept for Information Operations" paper on 15 May 1998 to serve as a catalyst for discussion and research to focus on what

Information Operations will be required by their concept of Operational Maneuver from the Sea. It states

> "The Marine Corps warfighting philosophy of maneuver warfare seeks to shatter the enemy's cohesion through a series of rapid, violent and unexpected actions which create a turbulent and deteriorating situation with which he cannot cope. Marine Corps information operations support maneuver warfare through actions to deny, degrade, disrupt, or destroy the enemy commander's ability to command and control his forces".[21]

The concept covers the broad application of information operations at the operational and tactical levels to influence an enemy's power or achieve national objectives. It provides the basic framework of information operations for the marine air ground task force.

The Marine Corps is in a unique position. It must closely align itself with the defensive information operations conducted by the Navy to ensure interoperability requirements. It also must retain the flexibility and adaptability to conduct information operations independent of the Navy as well. These independent operations will probably closely resemble the Army's approach.

This is not meant to slight the Marine Corps' efforts at Information Operations. The Marines conduct Information Operations across the spectrum without calling the mission information operations. Visits by the Marine Expeditionary Unit support the CINC's theater engagement plan. The Marines are fully prepared to conduct civil-military operations.

Currently, the Marines have not organized any specific Information Operations units. They are resourcing Information Operations billets at the joint level with officers trained in traditional military skills. They realize the need for developing their own Information Operations schooling and organizational process and are in the process of studying options.

SOCOM

There are nine activities that have been designated as Special Operations missions. Of the nine activities, four support Information Operations missions. They are Direct Action, Strategic Reconnaissance, Psychological Operations, and Civil Affairs.

However, Information Operations are truly a part of all Special Operations missions. As a minimum, operational security, information assurance, and counterintelligence are integrated into all missions.

While there is a great deal of doctrine on PSYOP and Civil Affairs, there currently is no overarching Special Operations Information Operations Doctrine.[22]

USA

Most of the activities of Information Operations are not new to the United States Army.

TRADOC Pamphlet 525-5, Force XXI Operations, provided the framework for integrating Information Operations into the US Army. It was focused on providing a concept for the Army's role in joint, full dimension operations. It captured ideas from across the Army. It defined Information Operations as "continuos combined arms operations that enable, enhance, and protect the

commander's decision cycle and execution while influencing an opponent's".[23] To further expand the concept of Information Operations, TRADOC published TRADOC PAM 525-69, Information Operations.

The United States Army published FM 100-6, Information Operations, in August 1996. This first attempt to lay the doctrinal framework was a hybrid between theory and doctrine. It indicated three specific operations that contributed to gaining and maintaining information dominance: Civil Affairs, Public Affairs and Command and Control Warfare. None of these were new areas, but all had been thrust into the forefront during the 1990s. The doctrine did not specify who was responsible for what activity at what level, what pay off could be expected and was difficult for tactical commanders to visualize. Since there was virtually no information operations experience and no resources provided, the doctrine was left to local interpretation and integration.

However, it was a starting point. It generated discussion between the branches within the Army and with sister services. The manual also provided a framework to begin structuring organizations, agencies and functions to meet the requirements.

Across the US Army, efforts were made to integrate the new doctrine. It was interpreted differently throughout the US Army. Some viewed it as nothing new and just an

attempt to put a new spin on old functions. Many viewed the doctrine as technologically focused and associated Information Operations with computer warfare only. Interpretation and integration varied widely by functional organization and level. What was missing was a shared common understanding of FM 100-6, who was responsible for what aspects of it, and who was responsible for the doctrine overall.

The Initial Draft FM 100-6, dated 30 April 1999, is a collection of tactics, techniques and procedures. It is less theory and more defined doctrine. One of the major changes is realigning Army Information Operations doctrine with the joint community and integrating lessons learned from Somalia, Bosnia, Haiti and various exercises. It also seeks to delineate responsibilities and establish a common understanding of Information Operations as it applies to US Army operations.

To resource the integration of Information Operations and to begin developing expertise, the US Army stood up the Land Information Warfare Activity (LIWA) at Fort Belvoir. The mission statement of LIWA is to "provide information warfare and information operations support to the land component and major/separate Army commands, active and reserve component, to facilitate planning and execution of information operations". Their purpose is "to provide Army commands with technical expertise that is not resident on the command's general or special staff".[24]

To accomplish eighteen different functions it is charged with, LIWA must interface with over forty different agencies within the Department of Defense. It serves as a conduit from the operational army to the institutional army. To support Field Commands, LIWA provides Field Support Teams to assist in planning Information Operations, vulnerability assessment teams (Red Teams) to identify needs of supported commands, Computer Emergency Response Teams to provide information assurance activities, modeling and simulation development, and sensor reprogramming. To accomplish these missions across the Army, LIWA has approximately 240 personnel assigned.

At the Headquarters, Department of the Army, the office of DAMO-ODI integrates Information Operations throughout the Army staff. TRADOC formed the Space and Information Operations Directorate (SIOD).

Officer Professional Management System XXI has created a new career field designated Functional Area 30, Information Operations. The purpose of this new career field is to "respond to the battlespace opportunities and challenges of accelerating growth in information dissemination capabilities supported by emerging information technologies. Information Operations Officers integrate efforts to protect the force's command, control, intelligence, surveillance and reconnaissance and other Information Operations capabilities". IO officers "coordinate, plan, integrate the execution of offensive and defensive Information Operations to gain information superiority in support of the commander's concept of the operation. IO is integral to every phase of Army and Joint planning operations".[25]

The Army is integrating information operations into the institutional school systems. The Army War College has successfully integrated it into their curriculum. The Command and General Staff College is working towards this end as well. Land Information Warfare Activity runs courses to train personnel at all levels the fundamentals of Information Operations and prepares instruction tailored to units it supports.[26]

Currently under revision, the Army's capstone FM 100-5, Operations, will contain an entire chapter on Information Support. The concept of Information Support incorporates Information Operations with information management to better support the warfighter. The manual envisions Information Operations as a critical enabling function for all Army operations.

IV. Systems Approach

In his book, *In Pursuit of Military Excellence*, Shimon Naveh applies the definition of a system to the operational level of warfare. The system, a complex of interacting elements, can be open to influences from its environment, or closed in which case no interaction takes place. The interaction of the system with its environment and among its parts is non-linear. It comprises three parameters: quantity, dominance of the system's aim, and quality. The quantitative parameter is the number of elements within the system. The dominance of the aim focuses the system and how it functions. As Naveh states

> "It is the actual definition of the system's aim that indicates the focus of tension between the system and its rivals and the direction for releasing its internal stresses...it is the abstract exposition of the aim that provides the system with its unifying determinant. The acute importance of this cognitive unity derives both from the natural tendency of the elements to split from the system and from the fact that perpetuating cohesiveness within the system guarantees its self-regulating ability, which in turn, enables the system to overcome the turbulence of external disturbances... moving the system from a state of abstract, cognitive commonality to a practical course of positive progress can only be achieved by translating the overall aim into concrete objectives and missions for the system's individual components".[27]

The last parameter, qualitative, refers to the synergy created by the elements.

Applying this construct to information operations builds a picture of information operations at the operational level. All military, political and social structures can be viewed as systems. Limited by technology, traditional military thought processes tend to focus on the parameters of a system individually. With the increasing value of information and emerging technology, the parameters of the system can be attacked simultaneously.

As the operational level of warfare is the bridge from the strategic objectives to the tactical actions, Information Operations focuses on denying the adversary freedom to use information to make decisions or use information as required by his systems to function properly. Whether the adversary is an operational commander, another nation-state, a tribal leader or a narco-terrorist, his ability to accomplish his objectives

depends upon the coordinated use of information. "Information is the lifeblood of any command and control system."[28] Denying, deceiving, degrading or disrupting the adversary's information enhances the application of lethal military power because he cannot react in time, space or through combat power in an appropriate manner. Conversely, protecting one's information becomes critical to ensure freedom of action.

This critical aspect is the effect of shock to the system. Shocking the adversary to degrade his ability to react to changing situations enables commanders to manipulate force ratios, timelines, and space to their advantage. Naveh's description of shock provides an excellent example of Information Operations when he states

> "Since operations constitute the consequence of the performance of military systems, which are goal-oriented in principle, it means depriving the rival system of its ability to attain its goal reflects the negative aspect of one's own aim. Moreover, separating the system from its brain and heart, both cognitively and physically, will inevitably lead to its disintegration and collapse".[29]

Use of the systems approach enables military planners to view the adversary's information requirements and flow as a system. This enables the planner to dissect it and determine what information is critical to the adversary, how best to affect a desired outcome on the information or

the flow of information at a critical time in space. By affecting the information, shock is introduced and multiplies the effects of other forms of power applied against the adversary. Naveh sums this up by stating "The dividing strike disrupts the basic operational mechanism (synergy) and breaks down the system's 'whole' into its independent parts".[30]

While commanders seek shock in combat operations, the systems approach expands when applied to stability and support operations. Information and its conveyance may be the endstate of operations in itself. Deterrence is an example. Combatant commanders' theater engagement plans are forms of information operations campaigns. By assessing what information to convey, what methods to employ and what the message is, the CINCs' seek to shape the information environment within their regions.

If warfare seeks to make a better peace, then utilizing an Information Operations systems approach becomes critical enable post-hostility success. By understanding the conflict and the adversary's information environment, a CINC may convey messages consistent with the desired political and military endstate throughout the spectrum of conflict.

V. Analysis

The evaluation criteria to analyze if joint and service Information Operations Doctrine is adequate are

relevancy, jointness, sustainability, and force integration. After defining the terms of evaluation criteria, each will be applied in context to current doctrine by using Naveh's systems approach.

Relevancy

In relation to Information Operations doctrine, there are three critical measures of relevancy. The first is timeliness, the second is application across the entire spectrum of conflict and the third is measures of effectiveness.

The Information Operations doctrine process is critically slow. While no reflection of Information Operations itself, the current doctrine process is inflexible and untimely when dealing with the velocity of technology and the dynamic world situation.[31] Doctrine is "the distilled insights and wisdom gained from our collective experience with warfare".[32] As an average in the joint and service doctrine processes, manuals are updated approximately every seven years. Currently, seven years of technological development triples the processing speed of commercially available computers.

This creates increasing tension at the operational and tactical levels of war. Information Operations technology, tactics and techniques can be developed, fielded, employed, and countered before the doctrine has had a chance to be updated.

Timeliness must also address emerging threats and provide enough flexibility to accommodate them. Most potential adversaries understand that the United States

Armed Forces will be difficult to defeat symmetrically. Potential adversaries will seek asymmetrical means to challenge their perception of United States strengths and weaknesses. As a Chinese military officer writes, "The supremacy of information will replace the supremacy of forces and weapons and will be the key in winning the upper hand".[33]

To be relevant, Information Operations doctrine must provide enough flexibility to cover the spectrum of operations from peacetime engagement and deterrence to fighting and winning the nation's wars. Given the growing emphasis of applying military power in operations other than war, Information Operations plays an increasingly critical role in peacetime engagement, deterrence and conflict prevention. Despite this, most doctrine at the operational and tactical levels focuses on Information Operations in combat operations.

Due to the technical nature of their services, Navy and Air Force doctrine highlights this by their sole focus on information warfare. As their first generation Information Operations doctrine is an evolution of their command and control warfare, this will improve as their doctrine process captures and consolidates lessons learned from recent operations. Until that point, their doctrine

is incomplete and does not link Information Operations across the full spectrum.

The US Army doctrine provides robust Information Operations doctrine at the tactical level across the spectrum. At the operational level, the doctrine does not lend itself to a clear understanding of organizational capability and responsibility. This is partially due to the Army's focus on providing the preponderance of its focus and effort on the tactical fight.

The third aspect of relevancy is the ability to show what benefit is gained by conducting Information Operations. This is truly the hardest and most fundamental problem. How does a commander know when he has gained information superiority and what that affords him to accomplish? Can the disruption of the adversary's information be measured in terms of combat power? The US Military has traditionally relied upon methods that provide feedback when employed. As a whole, there is a lack of standardized measures of effectiveness throughout the Information Operations arena.

By not being able to equate in quantitative terms what Information Operations can accomplish, commanders, staffs and planners at all levels are very cautious of placing too much emphasis on it. As an example of this, a recent CINC-

level exercise stressed deterrence and if deterrence failed, pursue combat operations. All exercise participants understood that regardless of how effective the deterrence was, combat operations would ensue. Despite Information Operations having its greatest impact during deterrence, there were no overall measures of effectiveness and little feedback if the deterrence missions were successful. While acknowledging the fine line, if commanders, staffs and planners do not receive proper feedback and are shown the relevancy of Information Operations, there will be little incentive to incorporate it.

Jointness

Since the Department of Defense term of joint is limited to the activities of two or more services working together, the term synergy is more applicable for joint Information Operations. Joint Publication 3.0 defines synergy as "integrating and synchronizing operations in a manner that applies force form different dimensions to shock, disrupt and defeat opponents".[34]

Joint and service doctrine addresses synergy both directly and indirectly in broad terms but do not develop a

cohesive process to achieve it. While part of this is due to the services developing their doctrine prior to the publishing of the first joint publication, it is also due to a difference by all involved in their approach to Information Operations.

Joint Publication 3-13 states that Information Operations can be a campaign by itself in peacetime and in deterrence and conflict prevention. The Navy and Air Force doctrines tend to focus on establishing and maintaining a level of information superiority akin to air or naval supremacy. The Army envisions Information Operations as an enabling function in support of military operations.

Given the varying approaches, joint Information Operations doctrine does not clearly address the issues of simultaneity, depth and shock. Each service's doctrine does, but none account for what its sister services will endeavor to accomplish at the same time with Information Operations, and how each can benefit from each other.

Kosovo is an excellent example. By eliminating the ground invasion option, a great many options for conducting Informational Operations at all levels was eliminated. By maintaining the threat of an invasion, the issues of simultaneity, depth and shock would have been exponentially

multiplied and would have presented the Serbian leadership with a greater and more credible threat.

Because of the probability that United States Armed Forces will continue to be employed as a member of coalitions, Information Operations doctrine must be explored at the multi-national and coalition levels. This is currently done on an ad hoc basis during crisis planning.

Currently, there is also a tension between the broad terms and guidance of Information Operations at the strategic and operational levels and the tactical actions required to carry them out. The services' tactical Information Operations doctrines are well established and designed to meet their specific service needs. It is difficult for joint or operational level Information Operations staffs to articulate the synergistic effects desired beyond traditional applications of military power.

Integration

To achieve synergistic effects, the Information Operations process must be integrated into the United States Armed Forces system. Integration is defined as the act of blending into a functioning whole.[35]

The Kosovo Crisis provides an opportunity for reviewing the doctrinal integration of Information Operations. As the commander of Joint Task Force Noble Anvil during the crisis, Admiral James Ellis stated Information Operations has "incredible potential" but is "not yet understood by warfighters".[36] This reflects the shortfall of integrating Information Operations early in the overall planning process.

This can be attributed to a number of factors. The first is Information Operations is new doctrine and requires time to firmly established in the planning process. The second is that there are few personnel who truly understand and are able to integrate Information Operations into the planning process.

In many ways, integration is the reverse of the timeliness criteria. The more changes and updates that are made, the harder it becomes to integrate Information Operations across the spectrum. This presents a challenge to doctrine developers and executors alike. Organizations like the Air-Land-Sea Application Center are charged with closing this gap by publishing multiservice tactics, techniques and procedures but are resource constrained.

Kosovo provides examples that the delineation of Information Operations responsibilities in planning and

integrating operations has not been worked out. While the Joint Chiefs of Staff are charged with the integration of Information Operations at the strategic level, it was the operational planners at European Command who did most of the planning. Despite the advent of JTF Noble Anvil standing up the first JTF Information Operations Cell, it was done on an ad hoc basis. To complicate matters, the approval process was unclear and most of the Information Operations tools available were not integrated into the plan. This enabled the Serbian leadership to take advantage and exploit of interior lines of Information Operations.[37]

Sustainability

Is Information Operations a fad? Is it a buzzword? The true measure of a doctrine is the resources applied to develop, integrate and maintain its relevancy. While there is a tremendous amount of discussion and debate about Information Operations across the services, each is applying resources in a different way.

By establishing a career field for officers in Information Operations, the Army is providing a first step for the application of resources. It will be incumbent

upon these officers to identify what direction the Army should take doctrinally and what resources are required. They will serve on division, corps and army level staffs as well as in agencies and organizations like LIWA throughout the Army. A great deal will depend upon their ability to identify shortcomings of Information Operations doctrine, equipment requirements and resources.

In contrast, the Navy and Air Force have not established a career field for Information Operations but are using it as extension of their command and control warfare. However, they are applying more resources to establish organizations to perform Information Operations.[38] Again, their application of resources tends to focus on the technical nature of Information Operations.

Applying the Systems Approach

By using Naveh's systems approach, the interaction and effects of all the evaluation criteria can be exhibited.

The quantity parameter is provided by the agencies, units, personnel and functions required to perform Information Operation as per doctrine. This reflects the sustainability criteria. Are resources being applied to the Information Operations doctrine to enable the process to identify the shortfalls and determine the proper resources required? An excellent example of the quantity criteria is the limited number of EA–6B Prowler radar jamming aircraft. Faced with two simultaneous small-scale contingency operations in both Iraq and Kosovo, there were barely enough aircraft to accomplish the mission requirements while retaining

a reserve for training and possible major theater of war operations. If the resources are not applied, the quantity will not support the requirements of the system.

The quality parameter is a reflection of relevancy, integration, and jointness. Before commanders integrate Information Operations into their concepts of operations, they must understand what they want it to accomplish for them. They must have confidence in the measures of effectiveness across the entire spectrum of Information Operations. The commanders' staff and planners must have an appreciation of how the joint and sister service Information Operations will benefit their operations and how to derive synergy from that. Information Operations must be integrated to ensure all levels of operations support each other and provide the correct information at the proper time to the right personnel. Again, this is intertwined with the quantity parameter to ensure the right number of trained personnel with the proper equipment to facilitate this action. Admiral Ellis' statement "Great people…with great access to leadership...but too junior and from the wrong communities to have the *required impact* on planning and execution" is a current reflection of the quality of current Information Operations and its application.[39]

The last parameter is the aim of the system. Given the difference of the joint and services approaches, the Information Operations aim stated at each level is subjected to interpretation based on what quantity is available, what quality the commander, his staff and planners place on it and the aim of what they want it to accomplish. Without the unifying aim, the system will naturally become many systems attempting to achieve the same ends but by different means.

VI. Conclusions

Information Operations is a complex function of every military operation. The doctrine must reflect the realities of the experience gained and the effort required educating, resource, planning and executing Information Operations.

It must explain that Information Operations increase in complexity and magnitude from the tactical level to the strategic level. Information Operations doctrine must address that this complexity and magnitude are subjective and each component of the system will view the value of information differently. It must provide a common basis for all military to use as a point of departure. It must build a picture of relevancy and utility in commanders' minds and be able to be expressed in their concepts of operations. It must provide a framework for translating difficult political objectives into military action with all means of force, lethal, non-lethal and informational.

While Information Operations Doctrine is adequate, there are several issues to address before the doctrine can be understood by the joint level and each service component, integrated and provide for synergy it is capable of generating.

Issues and Recommendations

The first issue is current doctrine does not clearly limit the magnitude and depth of Information Operations. The delineation of Information Operations as an enabling function or as a military operation in itself is vague. Taken literally, it is too broad and all encompassing. Since all military operations begin and end with an information component and physical destruction is a component of Information Operations, all military operations undertaken are essentially information operations.[40]

A recommendation is to lay out what defines an Information Operation as such and what varying degrees of Information Operations are found in every military operation. The doctrine needs to form a better picture in the mind of commanders and their staffs at all levels and across the spectrum of operations as to when Information Operations is the driving method to achieve the endstate and when it is an enabling function of combat operations. This clarity must reflect the different approaches, capability and flexibility each service offers.

The second issue is an extension of the first issue. Current Information Operations doctrine is vague about what the difference is at each level of war. There is a tremendous difference to a tactical ground component commander in combat operations and to a naval commander conducting a show of force as part of deterrence as to what Information Operations means and is to accomplish.

Each service doctrine provides a framework for its tactical Information Operations. The Air Force and Navy focus on the information warfare aspect of Information Operations. The land component forces by their very nature must focus on Information Operations across the entire spectrum. While both the Army and the Marines continue to refine what Information Operations The joint doctrine must provide a framework at the operational and strategic levels for all components to integrate their tactical doctrine and derive synergy across the spectrum of military operations. By providing this, joint commanders can integrate Information Operations more effectively into their concepts and intents.

Delineating responsibilities and lead agencies for each function or component of Information Operations Doctrine is the third issue. Who is responsible for training deception in the Army? Navy? By understanding who is responsible, others can seek information or affect coordination. The absence of doctrinal responsibilities means that area of doctrine will not have a proponent to champion its cause.[41] It also leads to duplication of effort, parochialism and not sharing lessons learned.

By identifying the above issues, the forth issue emerges. What information, from a doctrinal perspective, should flow through the Information Operations system? How does Information Operations deconflict traditional duties and responsibilities overall? While each service and command will specify exactly what they require, a framework to provide the basic structure will enable discussion and refinement of the current doctrine. The current trend to identify this flow is ad hoc (the absence of doctrine) during crises. A doctrinal framework addressing the flow from NCA down through all the components and

functions of Information Operations would enable personnel at all levels to identify what information they may need but did not know existed.

By identifying the characteristics of Information Operations at the different levels of war, who is responsible for them and how they interact, a clear system emerges and can be built upon. It allows quicker comprehension of the process and informational flow in times of peace, conflict and war. While this recommendation sounds simple, it enables personnel from any military organization to quickly identify where they fit in, how Information Operations should support them and how to become part of the information flow.

The clash of ideas forms the fifth issue. Each service has its own vision of Information Operations and how it is best applied to their ideal problem. None provide examples of how they would support other services or how other services would support them to develop synergy. Worse, the joint doctrine is an amalgamation of all ideas and does not truly lend itself well to a centralized vision.

Each service must state and integrate what Information Operations conditions it requires during operations. For one service to state a specific set of conditions without synchronizing it with another is to miss synergistic opportunities and risk duplication or interference of effort. Doctrine must reflect this.

Planning for Information Operations is the sixth area doctrine must greatly improve upon. If integrating Information Operations into military operations must be accomplished early in the planning cycle to achieve the proper effect, doctrine must provide a process to achieve this end. Avoiding the checklist mentality, Information Operations must be integrated into the doctrinal military decision making models of all the service.

functions of Information Operations would enable personnel at all levels to identify what information they may need but did not know existed.

By identifying the characteristics of Information Operations at the different levels of war, who is responsible for them and how they interact, a clear system emerges and can be built upon. It allows quicker comprehension of the process and informational flow in times of peace, conflict and war. While this recommendation sounds simple, it enables personnel from any military organization to quickly identify where they fit in, how Information Operations should support them and how to become part of the information flow.

The clash of ideas forms the fifth issue. Each service has its own vision of Information Operations and how it is best applied to their ideal problem. None provide examples of how they would support other services or how other services would support them to develop synergy. Worse, the joint doctrine is an amalgamation of all ideas and does not truly lend itself well to a centralized vision.

Each service must state and integrate what Information Operations conditions it requires during operations. For one service to state a specific set of conditions without synchronizing it with another is to miss synergistic opportunities and risk duplication or interference of effort. Doctrine must reflect this.

Planning for Information Operations is the sixth area doctrine must greatly improve upon. If integrating Information Operations into military operations must be accomplished early in the planning cycle to achieve the proper effect, doctrine must provide a process to achieve this end. Avoiding the checklist mentality, Information Operations must be integrated into the doctrinal military decision making models of all the service.

The seventh and most critical problem is capturing the Information Operations process. Across the services and at the joint level, a great lessons learned are not being captured and shared. There are very limited mechanisms or processes to improve systematically the basis of knowledge of Information Operations. While each service has a small effort underway, the majority of training, development, execution and results are unobserved. The impact of not capturing these lessons learned at this critical stage of Information Operations Doctrine development is compounded by the transient nature of personnel filling the Information Operations billets at all levels. A solution is to create a Center for Army Lessons Learned type agency and database to capture and catalog these experiences.

Summary

Information Operations doctrine is challenging to write because of the rapidity of technology, it is difference every time it is employed, it means something different to each service and even within each service. Its complexity and ambiguity have enabled many to claim they understand it but, in reality, they only understand a portion of it.

Current doctrine does lay down a good framework and is adequate. However, it is first generation doctrine and must be improved upon. Every major operation undertaken since the Berlin Wall has had a major Information Operations Component. Joint and sister service doctrine must reflect the lessons learned and provide a clearer picture of Information Operations at all levels of war, in all situations and for all functions and components of Information Operations.

[1] Samuel Guthrie, "The So-What of Information Warfare" (School of Advance Military Studies, Fort Leavenworth, Kansas, 1995), Page 12.
[2] Thomas Friedman, The Lexus and the Olive Tree (Farrar, Straus and Gireu, NY, 1999).
[3] Information Operations is not just a military operation or function. It is affecting all aspects of society, government and the business world. Old rules are changing and the pace of change continues to accelerate.
[4] USN Naval Doctrine Publication 6 (1995), Page 7.
[5] Random House Collegiate Dictionary, page 985.
[6] An aspect which merits further study is the degree required by the United States Military to protect the freedom of information and its flow for the nation as a whole. What level or type of attack upon information necessitates a military response? Will this be included in future National Security Strategies?
[7] The increase of non-governmental international agencies is proliferating. Information Operations and Civil Affairs represent two functions which interface with these agencies.
[8] Carla Bass, "Building Castles on Sand: Understanding the Tide of Information Operations" (Airpower Journal, Summer 1999), page 32.
[9] Joint Vision 2010, page 2.
[10] CJCSI 3010.01, 10 Oct 96
[11] Joint Vision 2010, page 16.
[12] Information Operations targets information or information systems in order to effect the information dependent process, whether human or automated. To achieve success IO must be integrated with other operations (air, land, sea, space and special) and contribute to national and military objectives.
[13] JP 3-13, page vii.
[14] Bass, page 36.
[15] JP 3-13, page viii.
[16] JP 3-13, page GL-9. The study of the SIO review and approval process merits further study. There is discussion on how to organize SIO and who should control it. Options vary from creating a Single Integrated Operations Plan like

at STRATCOM to creating an Information Operations Unified Command.

[17] JP 31-3, page viii.

[18] Bass, Carla D, page 28.

[19] ibid.

[20] Lane, Randall C, page

[21] Marine Corps Combat Development Command, "A Concept for Information Operations" (Quantico, Virginia, 15 May 1998), page 1.

[22] This merits further study. The Information Operations combat multipliers available in the SOF communities are not well understood by conventional forces. The author observed many BCTP warfighter rotations where information did not flow freely between SOF and conventional forces, allowing the adversary a degree of freedom he could have been denied.

[23] TRADOC PAM 525-5, page glossary - 4.

[24] LIWA Mission Statement.

[25] DA PAM 600-3, Chapter 39.

[26] This are requires further study. Since Information Operations doctrine is new and responsibilities are still being delineated, institutionalizing the doctrine requires a more coordinated effort. Currently, the Combined Arms Center is responsible for the integration of Information Operations center throughout the US Army Training and Doctrine Command. It works closely with DAMO-ODI, and SIOD to this end. This process will take time.

[27] Shimon Naveh, In Pursuit of Military Excellence (Frank Cass Publishers, 1997), page 6

[28] USN NDP6, Page 7.

[29] Naveh, page 16-17.

[30] Naveh, page 17.

[31] Discussion with Doctor Schnieder, 26 Nov 99.

[32] Joint Pub 1, 10 Jan 95, page 8

[33] Michael Pillsbury, Chinese Views of Future Warfare (National Defense University Press, Washington DC, 1997), page 314

[34] JP 3.0, page 14.

[35] Merriam Webster's Collegiate Dictionary, Tenth edition, Springfield, MA ,1997, page 698.

[36] Admiral Ellis, AAR JTF Noble Anvil.

[37] Admiral Ellis, AAR JTF Noble Anvil.

[38] This contrast merits further study to determine how best to apply resources across the services. While all services run schools, which teach bits and parts of Information Operations, there is no authoritative school, which teaches

Information Operations across the spectrum and is widely accessible to all services.

[39] Admiral Ellis, AAR JTF Noble Anvil.

[40] Discussion with LTC Jeff Turner, 4 Dec 99.

[41][41] **Discussion with LTC Jeff Turner, 4 Dec 99.**

BIBLIOGRAPHY

Allard, Kenneth. Somalia Operations: Lessons Learned. Institute for National Strategic Studies, National Defense University, Washington, DC, Jan 95.

Barwinczak, Patricia M. "Achieving Information Superiority". Pages 36 - 43, Military Review, September - November 1998.

Bass, Carla D. "Building Castles on Sand: Understanding the Tide of Information Operations". Page 27 - 45, Airpower Journal, Summer 1999.

Bellamy, Chris. The Future of Land Warfare. St. Martin's Press, NY, 1987.

Bunker, Robert J. "Information Operations and the Conduct of Land Warfare". Association of the United States Army Institute of Land Warfare as reprinted in September - November 1998 edition of Military Review, Fort Leavenworth, Kansas.

Church, William. "Kosovo and the Future of Information

Operations". Center for Infrastructure Warfare Studies Website at Iwar.org. 10 Nov 99.

Combelles-Siegel, Pascale. Target Bosnia: Integrating Information Activities in Peace Operations. National Defense University, Washington, DC, 1998.

Dick, Sameul R. "The Operation Proponent for Information Warfare". Naval War College, Newport, Rhode Island, 14 June 1998.

Doyle, Kevin J. "Information Operations: A Look at Emerging Army Doctrine and Its Operational Implications". School of Advanced Military Studies, Fort Leavenworth, Kansas. 1995.

Ellis, James O. Commander of Joint Task Force Noble Anvil. "A View from the Top" After Action Briefing on Task Force Noble Anvil.

Friedman, George and Meredith. The Future of War. St. Martin's Griffin, NY, 1998.

Friedman, Thomas. The Lexus and the Olive Tree. Farrar, Straus and Gireu, NY, 1999.

Guthrie, Samuel A. "The So-What of Information Warfare". School of Advance Military Studies, Fort Leavenworth, Kansas. 1995.

Lane, Randall C. "Information Operations: A Joint Perspective". School of Advanced Military Studies, Fort Leavenworth, Kansas. 1998.

La Perla, Philip A. "Creating Information Knowledgeable Leaders Through Information Operations Education". US Army War College, Carlisle Barracks, Pennsylvania. No Date Posted.

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

Libicki, Martin C. What is Information Warfare?. National Defense University, Government Printing Office, August 1995.

Jensen, William J. "Information Warfare's Missing Quarterback: The Case for a Joint Force Information Warfare Component Commander". Naval War College, Newport, Rhode Island, 13 February 1998.

Joint Chiefs of Staff. "Concept for Future Joint Operations: Expanding Joint Vision 2010". Washington, DC: Government Printing Office, May 1997.

Joint Chiefs of Staff. Joint Publication 1: Joint Warfare of the Armed Forces of the United States. Washington, DC: Government Printing Office, 1995.

Joint Chiefs of Staff. Joint Publication 3-0: Doctrine for Joint Operations. Washington, DC: Government Printing Office, 1995.

Joint Chiefs of Staff. Joint Publication 3-13: Joint Doctrine for Information Operations. Washington, DC: Government Printing Office, 28 January 1998.

Joint Chiefs of Staff. "Joint Vision 2010". Joint Electronic Library, Joint Chiefs of Staff CD-ROM, December 1997.

Joint Chiefs of Staff. Memorandum on Implementation Policy for Joint Vision 2010. CJCSI 3010.01, dated 10 Oct 1997. Joint Electronic Library, Joint Chiefs of Staff CD-ROM, December 1997.

Marr, Patrick M. "Information Warfare and the Operational Art". Naval War College, Newport, Rhode Island, 12 February 1996.

Naveh, Shimon. In Pursuit of Military Excellence. Frank Cass Publishers, London, 1997.

Newell, Clayton R. On Operational Art. Center for Military History, United States Army, Washington DC, 1994.

Office of the Chairman, Joint Chiefs of Staff. National Military Strategy of the United States. Washington, DC: Government Printing Office May 1997.

Office of the Chairman, Joint Chiefs of Staff. Joint

Vision 2010. Washington, DC, Government Printing Office May 1996.

Pillsbury, Michael. Editor-in-Chief. Chinese Views of Future Warfare. National Defense University Press, Washington DC, 1997.

Rhodes, J.E. "A Concept for Information Operations." Marine Corps Combat Development Command Paper, Quantico, Virginia, 15 May 1998

Schneider, James J. "Black Lights: Chaos, Complexity, and the Promise of Information Warfare". Joint Forces Quarterly, Autumn 1998.

Stein, Jess. Editor-in-Chief. Random House Dictionary, College Edition. Random House Inc., 1975.

Swain, Richard M. Filling the Void: The Operational Art and the U.S. Army. US Army Command and General Staff College, Fort Leavenworth, Kansas.

Szafranski, Richard. "A Theory of Information Warfare: Preparing for 2020".

Toffler, Alvin. Future Shock. Bantam Books, New York, 1971.

Tukhachevskiy, Mikhail. New Problems in Warfare. US Army Command and General Staff College, Fort Leavenworth, Kansas, 1 Nov 1983.

Warner, Christopher G. Implementing Joint Vision 2010: A Revolution in Military Affairs for Strategic Air Campaigns. Air University Press, Maxwell Air Force Base, Alabama April 1999.

US Air Force. Air Force Doctrine Document 1, Air Force Basic Doctrine. Washington DC: Department of the Air Force, September 1997.

US Air Force. Air Force Doctrine Document 2-5, Information Operations. Washington DC: Department of the Air Force, 5 August 1998.

US Air Force. "Air Force Vision Statement". Joint

Electronic Library, Joint Chiefs of Staff CD-ROM, December 1997.

US Army. Army Vision 2010. Headquarters, Department of the Army, Washington DC, 1996.

US Army. Department of the Army Pamphlet 600-3:

US Army. Field Manual 100-6, Information Operations. Washington DC: Department of the Army, 1996.

US Army. "Mission Statement". Land Information Warfare Activity, Downloaded from www.fas.org/irp/agency/inscom/liwa/mission.htm on 10 November 1999.

US Army. Draft Field Manual 100-6, Information Operations. Center for Army Doctrine, Fort Leavenworth, Kansas, 1999.

US Army. TRADOC PAMPHLET 525-5, Force XXI Operations: A Concept for the Evolution of Full-Dimensional Operations for the Strategic Army of the Twenty-first Century. Fort Monroe, VA: HQ TRADOC, 1 Aug 1994

US Marine Corps. "Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore". Joint Electronic Library, Joint Chiefs of Staff CD-ROM, December 1997.

US Marine Corps. "A Concept for Information Operations". Marine Corps Combat Development Command, Quantico, Virginia, 15 May 1998.

US Navy. "Forward from the Sea". Joint Electronic Library, Joint Chiefs of Staff CD-ROM, December 1997.

US Navy. Naval Doctrine Publication 6: Naval Command and Control. Department of the Navy, Washington DC, 19 May 1995.

US Special Operations Command. Special Operations Reference Manual. CD Reference Manual Version 2.1, January 1998.

Weidner, James R. "The People Side of Information Warfare". Naval War College, Newport, Rhode Island, 14 June 1995.

Whitehead, YuLin G. "Information as a Weapon: Reality versus Promises". Air University Press, Maxwell Air Force Base, Alabama, January 1999.