The Friction of Joint Information Operations

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

Second Term AY 99-00

REPORT DOCUMENTATION PAGE

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
01-01-1995	monograph	xx-xx-1995 to xx-xx-1995

4. TITLE AND SUBTITLE The 8th US Army: A Case for Warfighting Unclassified	**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) Jones, John J. ;	**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME AND ADDRESS School of Advanced Military Studies US Army command and general staff college ft. leavenworth , ks 00000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS ,	**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION/AVAILABILITY STATEMENT
A
PUBLIC RELEASE

,

13. SUPPLEMENTARY NOTES
14. ABSTRACT warfighting
15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT Unclassified	b. ABSTRACT Unclassified	c. THIS PAGE Unclassified	Public Release	58	Fenster, Lynn lfenster@dtic.mil
					19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703 767-9007 DSN 427-9007

SCHOOL OF ADVANCED MILITARY STUDIES

MONOGRAPH APPROVAL
Major Charles N. Eassa

Title of Monograph: The Friction of Joint Information Operations

Approved by:

_____Monograph Director
LTC Peter Schifferle, MA, MMAS

_____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 May 2000

ABSTRACT

The Friction of Joint Information Operations By MAJ Charles N. Eassa, USA, 40 pages.

Joint Publication 3-13, Joint Doctrine for Information Operations was published in 1998 to provide clarity and guidance for conducting joint information operations. This paper seeks to answer if the doctrine proved sufficient at the Joint Task Force Level.

The formation of Joint Task Forces is normally done under time constraints and with limited resources. Joint information operations doctrine must provide a framework that enables a common understanding and approach to its integration with other capabilities the JTF will employ.

Outlining information's role throughout the levels of war and the requirement for information at the JTF level, this paper uses the hierarchy established by previous keystone joint publications to determine if the joint information operations doctrine expanded on the established framework. During this process, the friction caused by the focus of *Joint Publication 3-13* is contrasted against the hierarchical joint doctrine.

The study concludes that *Joint Publication 3-13* represents a new and very complex arena within joint doctrine. Driven by the lure of technology as a substitute for common understanding of operational art, it is not sufficient but serves a starting point for the continued enhancement of the doctrine for better facilitation.

Joint Publication 3-13 created a great deal of friction. The publication did not sufficiently clarify the role or the value of information across the spectrum of conflict. It did not link the national instrument of power called information to military information operations to provide unity of effort. There was no discussion expanding the fundamentals of operational art from the joint information operations perspective. Technically oriented, Joint Publication 3-13 did not provide guidance for JTF Commanders to include information operations in their intent statements, concept of operations, or commander's critical information requirements. These omissions contribute to the friction of integrating information operations into JTFs.

I. INTRODUCTION

Since the Gulf War, the explosion of technology has driven the increasing importance of information operations.[1] Many have heralded a perceived shift in military conflict from massive destruction to precision warfare enabled by technology.[2] In politics, the economy and the military, information superiority has become a buzzword.[3] Glamorized and highly touted, computer network attack (CNA) and computer network defense (CND) gain national headlines weekly.[4] Doomsday predictions herald an "electronic Pearl Harbor". The defense industry is continuously developing new high-tech systems that shoot better, can detect the enemy further out and faster, enable quicker flow data, and make war more efficient.

In this challenging environment, the United States Armed Forces face the possibility of conducting operations across the spectrum of conflict anywhere in the world. Threats to the interests of the United States are able evolve more quickly due to the impact of technology and the accelerating pace of change. No longer can the military focus only on military operations conducted in a major theater of war.[5]

In response to this changing climate, the Joint Chiefs of Staff published *Joint Publication 3-13, Joint Doctrine for Information Operations* in 1998. The publication stated that the

goal of information operations was to protect United States Armed Forces information and information dependent processes while denying an adversary the ability to freely use his information and information dependent processes. As the cornerstone for joint information operations, this publication provided the United States Armed Forces guidelines, linkage to hierarchy of joint doctrine, and established common understanding for the conduct of all information operations in support of joint forces.

Currently, there is 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.

This debate has created a friction that is particularly apparent at the Joint Task Force level. Is there sufficient information operations doctrine to support Joint Task Forces given the different approaches to information operations and the different degrees of understanding and integration? This paper analyzes the current joint information operations doctrine to answer this question.

Section I describes the role of information operations in a Joint Task Force. Section II exams current Joint information operations doctrine and approach. Section III analyzes the friction created by joint doctrine to compare and contrast this information to determine if there is tension, consistency, or balance at the Joint Task Force Level. Section IV proposes key considerations and issues at the JTF level to provide clearer navigation through the friction of joint information operations doctrine.

As the operational headquarters that bridges theater strategy to tactical action, JTFs are the lowest echelon level of command addressed in joint doctrine.[6] They serve as the focal point for integrating component capabilities, processes, and approaches to support the joint force commander's intent. As JTFs are formed to conduct operations across the entire spectrum of conflict, joint information operations doctrine must account for the complexity of modern warfare.

A JTF conducting information operations must be prepared to cover the entire spectrum of conflict from peace to post hostilities. As such, the JTF's information operations can not focus solely on high-tech capabilities enabling commanders to gain "information superiority" against potential peer or near-peer adversaries.[7] It must address the level of information and information systems, however complex or low-tech, that the JTF must affect in pursuit of its mission. If properly conducted,

information operations integrate the National Security Strategy's message from peacetime through crisis to post-hostilities while enabling a synergistic effect of all the capabilities a JTF brings to bear. For the early twenty-first century, the JTF is the instrument the United States Armed Forces will employ to handle crises. It is imperative that joint information operations doctrine is provides clarity and sound guidance not only by those under the information operations umbrella but commanders, planners, military strategists, and other staff officers.

II. INFORMATION OPERATIONS AND THE JOINT TASK FORCE

Despite all the hype about the revolution in military affairs and coming cyberwars, information operations is about control. Situational awareness, decision-making, and communicating those decisions to the executors form the basis of this control. This section establishes the role of information operations in a JTF and links current joint doctrine from the National Strategic Level to the JTF to provide continuity about information operations through the levels of war.[8]

Every political, governmental, societal, business, and military organization practice information operations in some form. With the explosion of mass communications and cheap, easy-to-use computers, collecting, processing, and disseminating information has become easier but the art remains complex. Time

and distance no longer have the informational delaying factor they did twenty years ago.

While there are a great deal of experts and technicians who can set up, maintain, or degrade an information system, the system must serve a higher purpose other than making information flow quickly. In the military, the person who determines this purpose is the commander. Just as the commander determines the approach he wants to pursue to accomplish his assigned mission, his responsibility is to provide the vision for the integration of information operations. He must articulate, based on his mission analysis, what information he wants to protect, what information he wants to project, what he thinks the adversary wants to protect, what information can friendly forces attack and what will the enemy try to attack. By stating this in the commander's intent and the concept of operations, the commander elaborates his guidance and vision for the integration of information operations.[9]

His staff provides the necessary work to take this guidance and produce feasible options. These options include affecting the adversary's ability to maintain control. Traditional options focused on the destruction of enemy forces or maneuvering to a position of advantage. As information operations is about control, information operations options target the adversary's ability to collect, process, and disseminate information at a time and location of the friendly forces choosing. This causes the adversary loss of control at a critical time while protecting

friendly forces against the adversary's attempts to do the same. If integrated with other friendly force activities, information operations can hasten the disintegration of the adversary's will and or capability to resist. The attack on an adversary's control can serve as an economy of force effort, be conducted during peacetime, serve to signal national intentions during crises, create conditions favorable to friendly forces, and countless other possibilities. It is not bound by the tight restrictions of the lethal application of munitions nor constrained by employment in declared war only.[10]

Once the option is selected, the staff is responsible for assisting the commander to maintain situational awareness, help him determine critical decisions, and help him maintain control by communicating the decisions to the subordinates. One way the commander does this is by approving the commander's critical information requirements (CCIR). The CCIR forms the basis unity of effort within the staff to identify resources and convey the information the commander needs for making decisions. As the integration of information operations is identical to all other staff functions, it must use this framework to become integrated and synchronized.

In *On War*, Carl Von Clausewitz stated that "war is merely continuation of policy by other means".[11] The National Security Strategy reflects the nation's goals for preserving peace and stability throughout the world.[12] While establishing the President

of the United States' national strategy objectives, most are stated in terms of national information operations objectives. *Joint Publication 0-2, United Action Armed Forces* stated "National Security Strategy is 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".[13] While identifying information as an instrument of national power, joint doctrine focuses exclusively on the military instrument of power and does not explore the relationship and impact between the two instruments of national power. This creates friction in joint information operations because of tension in translating broad strategic and political guidance into tactical action.[14]

From the guidance in the National Security Strategy, the Chairman of the Joint Chiefs of Staff publishes the Unified Command Plan which "provides guidance to all unified combatant commands; establishes their missions, responsibilities, and force structure; delineates the general geographic area of responsibility for geographic combatant commanders and specifies responsibilities for functional commanders".[15] The Chairman of the Joint Chiefs of Staff also publishes the National Military Strategy with the input from the service chiefs and the combatant commanders (CINCs) to provide advice to the President and the Secretary of Defense. In turn, the CINCs carry out their assigned missions within their areas of responsibility to meet the national

security objectives. While law and practice charge CINCs to ensure coordination and integration with the other instruments of national power, doctrine references the interagency process as the vehicle to accomplish this but does not provide specific examples.

At the national strategic level, information is used to convey a nation's intent, policies, objectives, and expectations. Targeted at multiple audiences through official and unofficial channels, the fundamental purpose of information at the national strategic level is to foster democracy, advocate humanitarian concerns, enable free trade, and deter conflict. Information is also the mechanism used to control the nation's resource to achieve these aims. In actuality, the United States Government conducts information operations every day.

At the theater strategic level, CINCs tailor information operations to fit their assigned missions. Perception management within the CINC's area of responsibility is the goal which enable regional stability, deters aggressive behavior, and promotes the interests of the United States. Captured in theater engagement plans (TEPs), ports of call visits, military to military contacts, and countless other methods, the CINC is actively involved in conducting information operations routinely in peacetime. As crises arise, information operations have their greatest impact conveying the national intent, determination, and military capability. An example, the use of flexible deterrent options (FDOs) encompasses information operations to convey specific

threats if the aggressive behavior is not halted while protecting critical vulnerabilities. Again, information is the medium to control these efforts, both through the communication of intent and command of the resources.[16]

To deal with crises, the Secretary of Defense or a CINC may constitute and designate a joint task force to accomplish a specific limited objective that does not require overall centralized control of logistics. The JTF may be established on either a geographic or functional basis. While there are a number of standing JTFs, this paper focuses on JTFs that are formed by geographical combatant commanders for temporary purposes in response to the threat of armed confrontation.[17]

The JTF commander is responsible for operational control over assigned and attached forces while making recommendations to the establishing authority for accomplishing operational missions. As the bridge from strategic to tactical, control is critical to planning, resourcing and directing tactical tasks to accomplish strategic goals. The commander is also responsible for establishing and maintaining a joint staff with appropriate personnel in key positions from each of the services or functional components represented in the JTF.[18] *Joint Publication 0-2, United Action Armed Forces* stated that the basic doctrine for Joint Staffs should consider “the composition of the forces and the character of the contemplated operations to ensure the commander’s

staff understands the capabilities, needs, and limitations of each component part of the force".[19]

Of critical importance, this demonstrates the requirement for the information operations cell to understand and link the national strategic and theater strategic information operations to the JTF commander's mission analysis, intent, and concept of operations. The information operations cell is formed from selected staff representatives, representatives from the supporting agencies and subordinate components. The cell "merges capabilities and related activities into a synergistic plan" and "coordinates staff elements and/or components represented in the IO Cell to facilitate the detailed support necessary to plan and coordinate IO".[20] The cell is shaped to fit the mission and integrates the command and control warfare cell as the basis for forming the information operations cell. In short, this cell which the JTF commander depends upon to assist him in conducting information operations planning may not be formed as a cohesive, functioning and well-rounded group during the initial stages of the JTF's planning process. Critical, this factor highlights the linkage between the intelligence preparation of the battlefield and interagency processes that information operations requires to form a cohesive unity of effort and the impact of time constraints, limited information operations staff experience, and the ability to integrate information operations throughout the JTF's planning effort. The JTF's information operations cell will

only plan and integrate what it is familiar with while working with the rest of the staff.[21]

While doctrine does not establish a link from the informational instrument of national power to the JTF, an implied task of JTFs is to establish some degree of control over the information environment concerning their assigned mission. Nor does doctrine provide a framework for organizing the informational battlespace. As *Joint Publication 3-13, Joint Doctrine for Information Operations* stated that information operations could be the main effort for a campaign or operation, failure to organize responsibility for information operations based on level and target causes great friction just as failing to properly delineate geographical responsibilities. Therefore, the information operations cell must assist the JTF commander and his staff to understand the value and different types of information within the bounds of their mission from the National Security Strategy through the CINC to the JTF itself.[22]

While determining the value of information is extremely difficult at all levels, the joint definition of information does not provide any resolution; it is too broad, all encompassing, and vague.[23] To complicate matters, unified action demands incorporating information from the interagency process as well as from external sources like the media, non-governmental organizations (NGOs) like the International Red Cross, and any

nation-state actors like coalition partners, neutral countries and potential adversaries.[24]

This raises tension within the United States Armed Forces. The friction stems from the military's desire to focus on the tactical problem of defeating the enemy's forces without the constraints or interference of outside actors or complications. The inclusion of external sources like the media or NGOs adds a greater level of complexity to the military equation. The United States Armed Forces are just beginning to integrate the complexities of the modern battlefield into training.

Information operations does not adhere to the traditional attrition and annihilation theories that seek to engage the enemy in battle and defeat him by means of military force on force combat. Unlike hierarchical publications, *Joint Publication 3-13* was not based on the practice or interpretation of theory and experience. There was no discussion on information operations lines of communications, culmination, or decisive points.

This point creates a great deal of friction because Joint Publication 3-13 did not provide a clear discussion on the levels of information operations and responsibility for organizing the battlespace. In this regard, JTF information operations cells must have a sound doctrinal-based framework that enables organization of battlespace, and rapid teaming to the hierarchical information operations links at the CINC and interagency level. This provides the JTF commander cohesive information operations

with connectivity to national strategic information operations from the inception of the JTF. With this established, JTF information operations seeks to prevent an adversary from conducting cohesive and supporting operations at all levels of war by affecting his information and its flow across all his instruments of national power.[25]

To do this requires a great deal of intelligence preparation of the battlefield and works best by attacking multiple vulnerabilities simultaneously to overwhelm the adversary's response capabilities. Information operations may be extremely hard to determine true measure of effectiveness of their impact. Integrated and synchronized with the JTF commander's intent and concept of operations, information operations create a synergistic effect that present the adversary more problems than he can handle, limiting his options while increasing and protecting friendly options and capabilities.

As *Joint Publication 3-13, Joint Doctrine for Information Operations* stated that information operations have their greatest impact in peace and the initial stages of a crisis, the role of information operations must be determined upfront by the CINC and his staff. This also sets the tone for how the JTF incorporates information operations from its initial planning stages to mission accomplishment to support the CINC's intent.[26] Under time constraints and often without complete guidance, the doctrinal

link between the IO cells on CINC staff and the forming JTF is critical in providing this.[27]

Another tension that merits further study is the CINC's perception of information operations. As information operations is a new component which affects all traditional aspects of the military instrument of power, each CINC must have different expectations.[28] Does the CINC view information operations as the main effort to establish an information condition or to coerce the adversary? How does the CINC see the battlespace in terms of information operations? How does he integrate the sequencing of information operations in time and space?

The JTF commander and his staff determine the role of information operations by conducting mission analysis in a crisis and time-constrained environment. Like the CINC and his staff, the JTF's understanding, experience, and expectations of information operations will vary widely based on service, region, and mission. The JTF must identify how the adversary collects, processes, and disseminates information at all levels and throughout all activities, military, and non-military, to support his ability to conduct and sustain operations. Is there an informational center of gravity, whether it is support from the adversary's populace or a fully developed integrated air defense network? Does the adversary have the capability to affect friendly information centers of gravity or the ability to degrade or deny friendly information requirements? Are there political

constraints or future military operations that limit the types of information that can be exploited?

Answering these questions builds a framework allowing the JTF to integrate information operations during the planning process. During the course of action development phase, the information operations cell plays an imperative role in coordination, synchronization, and integration process. The cell must understand what capabilities exist, what it may need but not have the ability to accomplish, how it can assist others in achieving their task and purpose, how the battlespace is defined and what information condition is critical to the successful accomplishment of the mission.[29]

This effort enables the JTF information operations cell to recommend the best information operations strategy to the commander. This strategy must appear in the commander's intent and the concept for operations. The context of the strategy must state if information operations are a supporting or a main effort. Assuming information protection is a constant in any operation, the commander must state clearly how he intends to shock the adversary by denying him critical information, if information serves as a force multiplier for setting a condition or a combination of both.

Information is the medium through which the JTF commander will ultimately determine the mission's success or failure. The results of his plan's tactical actions will create the conditions

enabling the commander to state whether his vision has been accomplished. Measured at the operational level by an informational condition, the JTF commander communicates this to his higher headquarters. While beyond the scope of this paper, information operations at the JTF level are essential for identifying the termination of conflict and the beginning of a sequel.

Identifying the value of information at the JTF level is essential to support commander's ability to use and convey his information and information processes freely to achieve his stated purpose while denying the adversary the ability to do the same. This emphasis on the value of information from the national level through the JTF is a key component of the JTF commander's intent and concept of operations. By identifying the value of information, organizing the battlespace for information operations, and providing the JTF commander with doctrinally sound information operations staff work, information operations play a critical role in JTF's mission accomplishment. Without this, the bridge from strategic goals to tactical action is not measured with the same value and unity of effort while best using the resources available – creating friction between the levels and the JTF's ability to integrate information operations.

III. CREATING THE FRICTION

The purpose of joint doctrine is to improve the combat effectiveness of the United States Armed Forces and provide clear guidance on the fundamentals of joint warfighting. Joint doctrine is written to reflect existing capabilities, is authoritative but not descriptive.[30] As joint doctrine is hierarchical and "provides a military organization with a common philosophy, a common language, a common purpose, and a unity of effort", reviewing the chronological publication of current joint doctrine provides a foundation to analyze if information operations doctrine is sufficient.[31] From this foundation, the friction between the hierarchy of joint doctrine and joint information operations doctrine becomes readily apparent.

1995

Joint Publication 0-2, United Action Armed Forces linked joint doctrine to the national strategy and provided policy, doctrine, and principles to govern the performance of the Armed Forces.[32] It stressed the keynote of unity of effort from the President of the United States down through the chain of command.

Joint Publication 1, Joint Warfare of the United States Armed Forces provided broad warfighting guidance for joint doctrine. Its guidance requires leader judgment in application. Pointing out that joint doctrine is neither strategy nor policy, *Joint Publication 1* lists the principals of war and their application,

the fundamentals of joint warfare, and defines the role of doctrine.

Detailing the nature of modern warfare, the publication stated that the "Armed Forces of the United States face the most challenging environment" due in part to the multifaceted missions required to maintain stability, promote deterrence and win in combat.[33] *Joint Publication 1* also stressed joint doctrine "deals with the fundamental issue of how best to employ the national military power to achieve strategic ends".[34] Compiled through experience and training, joint doctrine "offers a common perspective from which to plan and operate, and fundamentally shapes the way we think about and train for war".[35] This enables JTFs to apply the principles of war with a common understanding to achieve its operational objectives to meet the strategic goals.

Joint Publication 2-0, Joint Doctrine for Intelligence Support to Operations did not discuss directly information operations. As the primer for joint intelligence, it provided the principals, purpose, and nature of joint intelligence. It described the intelligence architecture, provided definitions, and operational concepts. The publication also stated, "Gaining and maintaining intelligence dominance enhances the joint force commander's (JFC's) flexibility by opening additional operational options".[36] Intelligence dominance is not explained nor linked to information dominance. The definition of information in *JP 2-0* is

not the same as in *Joint Publication 1-02, Department of Defense Dictionary and Associated Terms*.

While *Joint Publication 3-0, Doctrine for Joint Operations* did not specifically mention information operations either; there were numerous references to the value and importance of information in joint operations. It provided an excellent discussion on Command and Control Warfare. *JP 3-0* provided fundamentals principals for joint operations, guidance for planning joint operations, and principals and considerations for military operations other than war. In the discussion of operational art, it stated the concepts of employing synergy, simultaneity, and depth.

Synergy is achieved by "synchronizing the actions of air, land, sea, space, and special operations forces in joint and multiple dimensions" in a manner "to shock, disrupt and defeat" adversaries.[37] The synergy is closely aligned with the concepts of depth and simultaneity. Simultaneity is the application of friendly force capability "against the full array of enemy capabilities and sources of strength" to facilitate the enemy's collapse by giving him more problems than he can handle with his capabilities.[38] Depth is applied to space and time to destroy enemy potentials before they can be brought to bear, to shape future conditions, and may affect an adversary's decision cycle.

The framework of *Joint Publications 0-2*, *1*, *2*, and *3* formed the hierarchy from which all other joint publications uphold. It

is reasonable that joint information operations doctrine would expand upon the concepts and foundations outline in these manuals while focused on creating a common understanding across the joint community.

1996

Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare provided the basis for offensive information operations. As a revision of previous joint C2W doctrine, it sought to integrate technological developments as a force multiplier with established disciplines like psychological operations to create a synergistic effect. Capabilities focused; there was no discussion on information operations. Yet, the publication provided the foundation for the processes of offensive information operations.[39]

Joint Publication 3-53, Doctrine for Joint Psychological Operations established the organization, planning considerations, and process for integrating psychological operations (PSYOP). The publication provided guidance on establishing a psychological operations task force for the joint force commander. It does not discuss information operations or the link from Psychological Operations to the other information operations-type synergistic capabilities. As a component of C2W, it does not provide a clear link to either *Joint Publication 3-13.1* or information operations.

Adding to the friction, this failed to organize the battlespace and responsibilities.

1997

Joint Publication 3-54, Joint Doctrine for Operations Security sought to establish a process for identifying and protecting critical friendly information. Critical to information operations, the publication stated the overall purpose of conducting operations security is to "force the adversary commander to make faulty decisions based on insufficient information and/or delay the decision making process due to a lack of information".[40]

1998

To provide an overarching doctrine that dealt with the complexities of modern warfare, the Joint Chiefs of Staff published *Joint Publication 3-13, Joint Doctrine for Information Operations*. Torn between the technically oriented focus of C2W doctrine and the increasing compression of the levels of war on the battlefield, it was intended to provide clarity on the military implication of information, its use and the impact on operational art.

Joint Publication 3-13, Joint Doctrine for Information Operations was to be the keystone manual for information

operations.[41] It stated the fundamental of information operations "involve actions taken to affect adversary information and information systems while defending one's own information and information systems". Information operations are a "critical factor in the joint force commander's capability to achieve and sustain the level of information superiority required for decisive joint operations".[42]

To accomplish this, information operations comprised of offensive and defensive information operations. Both offensive and defensive information operations integrate assigned and supporting capabilities and activities to achieve the commander's objective. Offensive information operations assigned and supporting capabilities and activities include operations security (OPSEC), military deception, psychological operations, electronic warfare, physical attack/destruction, and special information operations. While not an inclusive list, other capabilities and activities required by the JTF may be included. Each of these is mutually supported by intelligence.[43]

The purpose of offensive information operations is to "affect adversary decision makers and achieve or promote specific objectives" conducted across the spectrum of conflict at all levels of war. Conducted in peace and the beginning of a crisis, they have their greatest impact and effect. Once the crisis becomes a conflict, offensive information operations can be a critical force enabler. *Joint Publication 3-13* implies that

offensive information operations could the focus of a campaign with combat operations in a supporting role.[44]

The principals of offensive information operations stated that the human decision making processes are the ultimate targets. Offensive information operations must establish clearly identifiable objectives which support overall national and military objectives. This must include measures of success. Activities by non-Department of Defense organizations may be integrated and deconflicted to support the JTF commander's offensive information operations.[45]

To accomplish this, doctrine requires several conditions be met. The first is developing an in-depth understanding of the adversary and how information operations can affect him. The second is to identify information systems value, use, and flow of information, strengths, and vulnerabilities. The third step is to determine the target lists that match the best attack system with the vulnerability presented and the measures of effectiveness to assess outcomes. The fourth step is to gain approval necessary. The fifth step is to integrate, coordinate, and implement the plan.[46]

Offensive information operations include perception management. The definition of perception management is "actions to convey and/or deny selected indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence

official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, OPSEC, cover and deception, and psychological operations".[47]

Offensive information operations may require the contribution of other activities to support the JTF commander's information operations objectives. Public Affairs are used to inform internal and external audiences. Internal audiences are defined as within the military organization and external is considered the public. Civil Affairs are employed to establish and maintain relationships between the JTF military forces and civil authorities. Offensive information operations can be conducted to support defensive information operations.[48]

Defensive information operations are constantly being conducted with the extent varying on the threat to the information environment. It conducted through OPSEC, physical security, counterdeception, counterintelligence, electronic warfare, special information operations, and information assurance. The purpose of defensive information operations is to protect and defend information and information systems.[49]

Four interrelated processes support defensive information operations. They are information environment protection, attack detection, capability restoration, and attack response. These processes, if coordinated and resourced, provide for the free flow

of information and the ability to assess, recover, and respond to an attack on friendly information or information systems.[50]

Information environment protection is protecting the United States Armed Forces ability to collect, analyze, disseminate, and use information freely. Primarily focused on information systems and facilities, it must also encompass decision-makers. Policies, procedures, and vulnerability assessments are tools to achieve the desired state of protection.

Information attack detection is the timely detection and reporting of an intrusion or attack. This is critical to enable capability restoration and attack response. Closely linked with other governmental agencies, detection and restoration are very technical and dynamic in response to the ever-evolving nature of technology. Attack response encompasses offensive information operations aspect.

Joint Publication 3-13 directs command and control warfare cells to be reconfigured to function as information operations cells. This cell provides the joint task force commander with the capability to integrate, coordinate, and deconflict information operations throughout the spectrum of conflict with his intent and concept of operations. The cell must be broad-based to incorporate joint, service, interagency, and multinational information operations capabilities.[51]

At the operational level of war, information operations are conducted to either achieve or support operation objectives.[52] The

JTF objectives may range from coercing an adversarial nation to cease hostile activities or threats to providing humanitarian relief following a natural disaster. Offensive and defensive information operations support the JTF to deter adversaries, and if required – fight and defeat the adversary at the least cost to the United States and friendly nations.[53]

As the foundation for information operations, *Joint Publication 3-13* contributed significantly to the friction by not clearly addressing the linkages to its hierarchical and supporting doctrine. Despite its cited purpose as the "guidance contained herein provides joint force commanders and their component commanders with the knowledge needed to plan, train for, and conduct IO", the publication did not sufficiently doctrinal lubrication for easing the friction it generated.[54]

IV. THE FRICTION

Did the publication of Joint Publication 3-13 provide clarity to the integration of information operations in JTFs or did it create a friction of information operations? This section compares and contrasts joint doctrine to determine if tension exists between the doctrine; if there is consistency throughout doctrine as applied to JTFs; and if it provides clear direction for the integration of information operations into joint warfighting.

While Joint Publication 1 elaborated on the fundamentals of warfighting, Joint Publication 3-0 further details this. As the "linchpin of the joint publication hierarchy", it provided guidance on the fundamentals of joint operations, planning for joint operations, joint operations in war, and military operations other than war.[55]

Joint Publication 3-13 does not expand on the foundation laid by its two hierarchical predecessors. Absent are the links from joint information operations to the organization of an operational area, key planning considerations, and operational art. This omission failed to serve the hierarchical doctrine ladder and build upon the established foundation.

The establishing CINC defines the joint area of operations (JOA) within his area of responsibility for the JTF commander. *Joint Publication 3-0* provided guidance to organize the JOA into joint special operations area, areas of operations for component commanders, combat and communications zones, and areas of interest. While facilitating operational command and control of traditional military functions, this does not delineate nor organize the battlefield for joint information operations.

At all levels of war, information operations of both friendly and adversarial forces are not bound by geographical or artificial limitations. In many cases like Somalia and Vietnam, the regional adversary can not match the overwhelming firepower and military resources but targets the will of the friendly political

leadership through the affects of information operations. As JTFs can be created for any contingency, the examples and discussion provided in Joint Publication 3-13 that did not cover the range of options at the operational level for this.[56]

It did not provide clarity for the JTF commander on the types of information he must protect outside of his immediate military informational requirements but allows him the latitude for determining this. What national level information or information processes must he protect? Joint Publication 3-13 stated that defensive information operations "integrate and coordinate protection and defense of information and information systems" without providing clarity to the levels or value of information.[57] Under time constraints and the pressure of standing up a JTF, doctrine should provide a starting point to facilitate proper planning and resource allocation to ensure unity of effort.

As mentioned earlier, the tension of the military focused on military functions is the gap is exactly the asymmetrical opening adversaries will exploit. In Kosovo, the adversary's information operations organization was able to gain and maintain the initiative by turning collateral damage incidents into international headlines. These informational attacks focused the Serbian informational national instrument of power against the United States and NATO informational instruments of power. Admiral Ellis, commander of Joint Task Force Noble Anvil during the Kosovo crisis, highlighted the failure of friendly forces to

capitalize on the Serbian ethnic cleansing campaign while allowing the Serbs to exploit the collateral damage issue.[58] The failure comes mainly out of the organization of the battlefield. Since responsibility for limiting or countering the Serbian national information operations from the outset was not clearly defined, the adversary was able increase the friction and friction by gaining and maintaining the initiative. Admiral Ellis stated that this alone double the length of the conflict and added great strain to the coalition.[59]

This highlights *Joint Publication 3-13*'s lack of addressing the approval process for informational weapons of war and tactics as another critical factor in the organization of the information operations battlefield. As computer network attack capabilities are very compartmentalized, how is the battlefield organized to deal with the second and third order effects of using such an attack technique? As informational weapons do not share the same direct cause and effect relationship of traditional weapons of war, is it a JTF's responsibility to handle the effects of these weapons or does the CINC retain control? *Joint Publication 3-13* implies for information operations planners at all levels to consider CNA during their mission analysis.

Joint Publication 3-13 did not explore or expand the key planning considerations of commander's intent, concept of the operations, and targeting. In translating strategic guidance into tactical objectives, JTFs play an essential role in determining

accomplishable military tasks to meet the stated mission. In a time constrained environment, doctrine is critical to assisting newly formed JTF staffs integrate and synchronize all aspects of combat power to provide maximum flexibility for the commander and limit the adversary's options.

Using the framework of the estimate process as an example, there is not a clear link or process to facilitate the integration of information operations into key planning considerations. During the Kosovo Crisis, Admiral Ellis pointed out while the right tools where in place; the information operations planners were too junior to have the required impact on the planning process.[60] As JTFs are stood up, this has a direct impact because junior information operations officers will not be able to gather the proper intelligence and geostrategic context required for conducting his information operations mission analysis. Joint Publication 3-13 did not address rank in the organization of the information operations cell. By not addressing this issue, junior information operations officers will be relegated to planning information operations solely as a limited enabling function for military versus military capability instead of incorporating the broad-based vision sought for the planning effort.

As recent crises have shown, this shortfall can provide an adversary with options to exploit. As the JTF builds overwhelming combat power, the adversary uses asymmetrical operations to gain the initiative. Although doctrine stated that information

operations have their greatest impact in the opening phases of a crisis, there is no discussion of what options information operations can generate or how to limit the adversary's. As there is no doctrinal process identified to preclude this, this establishes the tone for information operations for the duration of the crisis.

Centers of gravity, decisive points, and specific operational characteristics are essential to the estimate process. Discussed at length in *Joint Publication 3-0*, *Joint Publication 3-13* does not elaborate nor put these in an informational operations perspective. This omission contributes significantly to the friction by not linking the framework of information operations to doctrinal terms understood and employed throughout the planning process.

In the planning process, *Joint Publication 3-13* did not address determining the informational requirements two levels up (national strategic and theater strategic) or how it affects the JTF's operations. Although information operations may be the JTF's main effort, this manual does not suggest adding a clear and concise statement of information operations to the commander's intent nor writing a task-and-purpose type mission order for subordinate units.

The greatest contribution to the friction of information operations is linking information operations to operational art. As the function of information operations is new and doctrine is

based on theory and collective experience, the lack of discussion in doctrine on the operational art of information operations creates a vacuum. Using the fundamentals of operational art listed in *Joint Publication 3-0* of synergy, simultaneity and depth, anticipation, timing and tempo, and operational reach and approach serve to highlight the confusion brought by this omission.

The JTF employs synergy to combine its forces and actions to "achieve concentration in various dimensions, all culminating in attaining the objectives(s) in the shortest time possible" and "arrange symmetrical and asymmetrical actions to take advantage of friendly strengths and enemy vulnerabilities and to preserve freedom of action".[61] Synergy created by the combination of forces creates shock, disrupts, and denies the adversary freedom of action, causing a quicker breakdown in the enemy's capability to resist. Since the JTF must coordinate the contributions of air, land, sea, space, and special operations, information operations does not generate its synergistic effect if not integrated upfront with these functions. *Joint Publication 3-13* did not discuss information operations in terms of different functions and its support of them with the exception of the four aspects of information protection mentioned earlier.

Likewise, simultaneity and depth formed the foundations of deep operations. The object of simultaneity is to hit the adversary with more problems than he can handle to overwhelm his

capacity to command and control his forces, recover from the shock, and to cause disintegration. Depth can be used in terrain or time terms. Used properly, information operations integrated at the JTF level can target the strategic, operational and tactical levels throughout the depth of the battlespace, creating havoc in the military and non-military arenas to achieve paralysis. *Joint Publication 3-13* does not provide a framework for analyzing or a discussion on the concept.[62]

Anticipation is "key to effective planning".[63] Simply put, anticipation in information operations is a cause and effect relationship. If friendly forces do course of action A, the adversary has option x, y, and z available. The JTF IO Cell must anticipate information operations causes and effects to provide the commander options and limit or mitigate adversarial options. Anticipation is directly linked to situational awareness as well. If the cell has not anticipated what is within the adversary's capacity and will, they will be unable to maintain situational awareness and react to maintain the initiative. *Joint Publication 3-13* only discussed anticipation in the context of military deception and not about information operations overall.

Closely related to simultaneity and depth, timing and tempo provide another force multiplying power for the JTF commander. Currently, few adversaries can match the tempo the United States Armed Forces are capable of generating in conventional force on force combat. Timing is equally as important to sequence the

tempo in relation to friendly force availability and capability and the effects desired in time and space. *Joint Publication 3-13* presented a brief discussion on timing in planning and did not discuss tempo at all. While the publication stressed the importance of achieving and maintaining information superiority, the critical aspect of timing and tempo are omitted.

Operational reach and approach are interwoven throughout operational art and are linked directly to the organization of the battlespace. Integration of other elements of national power increase the operational reach and approach and create a greater unity of effort. Conversely, the operational reach of the adversary influences basing issues, force flows, and force protection. While *Joint Publication 3-13* emphasized the reach of technology and the impact it has, it did not discuss the issue of operational reach or approach. Critical to deterrence and the initial stages of a crisis when forces to respond may not be in place or within reach, the failure to link this fundamental to information operations degrades the publication's highlighted point about information operations serving its highest importance early in crisis evolution.

Another source of friction is the technically focused definition and application of information superiority. The definition is the "capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same".[64] Stated further, "JFCs

should have the capability to achieve and sustain information superiority over their adversaries".[65] Technically oriented, the process of developing and maintaining information superiority is not an endstate unto itself and does not link directly or indirectly to the defeat of an adversary.

Given the multifaceted missions a JTF may be required to conduct, *Joint Publication 3-13* does very limited guidance in dealing with information in low-tech crises. With the wealth of operational experience gained by the United States Armed Forces during the 1990s, very little has been captured in doctrine.[66]The friction of information operations is created by not adhering to fundamentals and by breaking the established hierarchical doctrinal linkage. While recognizing that *Joint Publication 3-13* represents new capabilities and considerations in joint warfighting, it must explain these concepts using a framework already established and understood. By not using the established framework, information operations remain enshrouded in friction, requiring tremendous effort to grasp the breadth of information operations and be able to translate them into an operational context that is understood by all warfighters.

V. EASING THE FRICTION - CONCLUSIONS AND RECOMMENDATIONS

Far from being an academic discussion, the friction created by *Joint Publication 3-13* strikes directly at the integration of information operations to support a JTF. New and unproved,

information operations doctrine is not built upon a foundation which appeals to warfighters. Since *Joint Publication 3-13* does not provide an operational view of how it links to the organization of the operational area, key planning points, and operational art while supporting the JTF commander and his staff, it is relegated to the IO Cell and integrated as an afterthought or in response to the enemy. By not providing links to the hierarchy of doctrine, information operations is seen as a stovepipe and only creates friction when introduced into planning under stressful situations like forming a JTF.

While *Joint Publication 3-13* stated upfront information operations "involve actions taken to affect adversary information and information systems while defending one's own", it focused mainly on the technological aspects of information operations.[67] Focused on the growing dependency of technology and assumes all potential adversaries share the same reliance and cultural values as the United States Armed Forces. This is reflected as *Joint Publication 3-13* lists the fundamentals of information operations as the integration of increasingly complex information systems.[68] In contrast, *Joint Publication 3-0* stated clearly that "understanding the cultural differences is important if friendly forces are to establish conditions necessary to achieve strategic goals".[69]

Joint Publication 3-13 is not sufficient for JTFs but does serve as an initial point of departure for the continued expansion of joint information operations. Instead of providing clarity and guidance, it generates incredible friction. Technically focused, *Joint Publication 3-13* is oriented on the flow of information and not on the decision-makers. The publication does not link the hierarchy of doctrine to information operations by complying with "the composition of the forces and the character of the contemplated operations to ensure the commander's staff understands the capabilities, needs, and limitations of each component part of the force".[70]

Nor does it provide for the link to operational art as laid out in *Joint Publication 3-0*. Without this foundation, commanders can not understand information operations at the JTF level, how it affords options while stripping the adversary's, and how it can be used against them.[71] As doctrine is derived from experience, JTF commanders are hard pressed to integrate capabilities and functions to enhance their own control while degrading their adversary's without this cornerstone to guide them.

This missing component is formed in part by the failure of joint information operations doctrine to create a common understanding. As each service has distinctly different tactical requirements, joint doctrine should identify these and serve as a common point of reference. This becomes more critical as

information operations at the strategic and operational level directly influence all operations, not just information operations, at the tactical level.

Just as the approach to joint information operations doctrine must encompass a common point of reference, it must not limit itself to focusing on the flow of information rather than what that information is supposed to do and how to maximize or degrade the combat potential from it. The doctrine can not afford to ignore low-tech challenges to the United States Armed Forces and must account for information across the spectrum.

Doctrine must stand the velocity of change. To do this, it must be well founded in fundamentals. Joint information operations doctrine has to link with operational art. There are plenty of historical examples ranging from the deception operations conducted at all levels for the invasion of Normandy to Operation Just Cause. Without fundamentals, the doctrine will not stand the pace of technology and JTF commanders will be limited to integrating information operations from their personal or their staff's experience.

The doctrine must provide for the integration of information operations into the commander's intent and concept of operations. Just as operational fires are a tool the JTF commander can use to enhance his control and degrade an adversary's, so is information operations. This must include the complexities of the informational instrument of power to the military application of

information operations. This would go a long way to facilitate JTF commanders and CINCs' vision of integration of these two mutually supporting efforts. The synergy derived would provide great benefit in theater engagement plans and during the initial stages of crises.

In summary, joint information operation doctrine does not sufficiently support JTFs because it fails to provide a common picture with a common language to integrate the fundamentals of operational art. If information operations is to serve as a force multiplier for the JTF, than the doctrine must link to the hierarchy established and provide commanders and their staffs a cornerstone to build from. It can not create friction by failing to link to its hierarchy.

Endnotes

[1] Moore's Law of computer processing power stated that since 1990 commercially available memory and processing power double approximately every 18 months. Commercial personal computers bought in 1995 are hard pressed to run software designed in 2000. Likewise, businesses seek to "remain relevant" and not allow their competitors a perceived advantage by using old software and hardware.

[2] Waltz, Edward, *Information Warfare: Principals and Operations* (Norwood, Artech House, 1998) page 10.

[3] Information superiority is defined in Joint Vision 2010 as the ability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. Buzzwords and the concepts that drive them are an excellent topic for research. Given the American society's love for technology and disdain of mundane chores, certain organizations within the United States Armed Forces and the defense industry have tried to capitalize on the use of buzzwords and "buzz-concepts" to promote weapons systems and perceived requirements.

[4] The Melissa Virus and the Lovebug Virus are recent examples of the media's role in computer network attack and defense issues. Due to the impact both attacks had, international news agencies treated them like it would conventional attacks between nations. This requires further research to determine if a hacker operating independently or in collusion with others could really produce an "electronic Pearl Harbor".

[5] Joint Chiefs of Staff, *Joint Publication 1, Joint Warfare of the Armed Forces of the United States* (Washington DC, Government Printing Office, 1995) page I-1.

[6] Joint Chiefs of Staff, *Joint Publication 0-2, United Action Armed Forces* (Washington DC, Government Printing Office, 1995) page IV-9.

[7] This is a difficult topic within information operations. There is no measurable standard for gaining information superiority. Also, with the velocity of technology, determining what capabilities potential

adversaries may possess is complicated and very subjective. Given that technology has a lifespan of three to five years, joint doctrine takes about seven to ten years to be fielded and accepted by the services. There is ample research and information available on what the United States Armed Forces may face in 2010 based on technology but little acceptance as most tend to focus technical capabilities rather than the low-tech emerging threats.

[8] Control enables resources, manpower, will and direction. Without the ability to control its resources or effort, no nation, organization or military can accomplish its purpose.

[9] The recent devaluation of the new Internet stock market is a commercial reflection of this. Many dot-com companies were unable to prove worth greater than enabling the free flow of information. They failed to adhere to standard business fundamentals and consequently, were unable to sustain the turbulent market and loss of financial support. The debate over the "new" economy created by the impact of the Internet and technology is very similar to the debate within the United States Armed Forces over the impact of information operations.

[10] This is not to imply that there are no restrictions placed on information operations. This merely reflects that information operations can be utilized in a greater role than a tank or a frigate. Information operations are truly limited only by the approving authority and imagination.

[11] Carl Von Clausewitz, *On War*, ed. Michael Howard and Peter Paret (Princeton, Princeton Press, 1976) page 87. As policies are western governments' method of codifying information and conveying their intentions, Chapter One is indirectly written about information operations.

[12] In contrast to *On War*, the National Security Strategy focuses on maintaining stability, deterring conflict and if required – fight to win. *On War* focuses entirely on its title subject.

[13] Joint Chiefs of Staff. *JP 0-2*, I-2. The study of information operations at the national strategic level merits further research.

[14] While this subject is of great merit, it is beyond the scope of this paper.

[15] Joint Chiefs of Staff. *JP 0-2*, xvi.

[16] There are many articles written about creating an Information Operations CINC. Theater Engagement Plans are new and there is very little information available about them in joint doctrine. Theater Engagement Plans offer an opportunity to create synergy with interagency information operations.

[17] Joint Chiefs of Staff. *JP 0-2*, IV-10.

[18] Ibid., IV-11.

[19] Ibid., IV-11.

[20] Joint Chiefs of Staff, *Joint Publication 3-13, Joint Doctrine for Information Operations* (Washington DC, Government Printing Office, 1998) page IV-2. JP 3-13 provides a doctrinal layout of actors and responsibilities of the IO cell. What it does not provide is guidance to provide that cells a common focus given the time constraints in forming a JTF and the diverse nature of the cell participants.

[21] Outside the scope of this study but an area that requires further study, the issue of rapid team the JTF information operations cell bears great impact upon the integration of joint information operations doctrine. While each CINC maintains a Deployable JTF Augmentation Staff and the Joint Information Operations Center has deployable information operations augmentation support teams, a JTF staff will fundamentally focus on what operations and doctrine it is comfortable with and will resist or have friction with outside agencies' recommendations during stressful and time-constrained conditions.

[22] Ibid., II-1. There is very little information (no pun intended) on the types of information and their values. While several attempts have been made to codify the value of information and the environments in which the JTFs will operate in, the closest the author has come across in the pursuit of this research was the general systems theory in Shimon Naveh's *In Pursuit of Military Excellence*.

[23] Ibid., I-9. Information is defined first as facts, data, or instructions in any medium of form and second as the meaning that a human assigns to data by means of known conventions used in their representation.

[24] This area warrants further study. With the exception of total war, there will be a plethora of non-state actors involved in any given operation. These organizations normally have a better understanding of the cultural aspects of the crisis and can provide critical insight on the role of information.

[25] Robert Leonard, *The Art of Maneuver* (Novato, Presido Press, 1997) page 19. The Author provides great insight to the United States Armed Forces' homage to the religion and lure of firepower. While no military operation is easy, the United States Army Combat Training Centers model for the mid-1990s is an excellent example of this mindset. The focus was on the tactical problem of force on force only.

[26] Another tension that merits further study is the CINC's perception of information operations. As information operations is a new component which affects all traditional aspects of the military instrument of power, each CINC must have different expectations.[26] Does the CINC view information operations as the main effort to establish an information condition or to coerce the adversary? How does the CINC see the battlespace in terms of information operations? How does he integrate the sequencing of information operations in time and space?

[27] Joint Chiefs of Staff, *JP 3-13*, viii.

[28] As much as any professional military officer, CINCs are the product of their environment. Within each service, there is great debate on what information operations means to that particular service and what it should accomplish in the joint arena. For example, The United States Air Force accepts information operations as a main effort but the United States Army views it as an enabling function.

[29] This critical area merits further research.

[30] Joint Chiefs of Staff, JP1, vi.

[31] Joint Chiefs of Staff, *Joint Publication 1-01.1, Compendium of Joint Publications* (Washington DC, Government Printing Office, 1998)

[32] Joint Chiefs of Staff, *JP 0-2*.

[33] Joint Chiefs of Staff, *JP 3-13*, vii.

[34] Joint Chiefs of Staff, *JP 0-2*, I-2.

[35] Ibid.

[36] Joint Chiefs of Staff, *Joint Publication 2-0, Joint Doctrine for Intelligence Support to Operations* (Washington DC, Government Printing Office, 1995) page vii.

[37] Joint Chiefs of Staff, *Joint Publication 3-0, Joint Doctrine for Operations* (Washington DC, Government Printing Office, 1995) page III-11.

[38] Ibid., III-12.

[39] In the author's opinion, JP 3-13.1 is technically oriented and focused on achieving superiority through electronic warfare and scientific means as opposed to emphasizing other softer, unquatifiable force enablers like PSYOP. As such, its technically oriented nature has heavily influenced the integration of information operations and its doctrinal development. Beyond the scope of this paper, this area merits further research.

[40] Joint Chiefs of Staff, *Joint Publication 3-54, Joint Doctrine for Operations Security* (Washington DC, Government Printing Office, 1998) page I-3.

[41] The United States Navy and Air Force are strong supporters of the C2W doctrine. It forms the basis for their approaches to information operations. This also reflects their services technical nature and orientation.

[42] Joint Chiefs of Staff. *JP 3-13*, II-10.

[43] Ibid., II-2.

[44] Ibid., viii.

[45] Ibid.,I-3. This would preclude emergent strategies. It also reflects *JP 3-13* lack of discussion on generating options for the commander.

[46] Joint Chiefs of Staff. *JP 3-13*, II-2.

[47] Ibid., GL-9.

[48] Ibid., I-10.

[49] Ibid., GL-5. The definition of counterdeception is efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. The information operations component of counterdeception does not include the intelligence function of identifying foreign deception operations. The definition of counterintelligence is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. Joint doctrine is unclear as to what are the bounds between traditional intelligence functions and activities and information operations.

[50] Ibid., Chapter 3.

[51] Ibid., Chapter 1 discussed at length the implications and considerations information operations planners must understand at all levels of war across the spectrum of conflict.

[52] Ibid., I-2.

[53] Author's opinion.

[54] Joint Chiefs of Staff, *JP 3-13*, Chairman's Remarks on cover insert.
[55] Joint Chiefs of Staff, *JP 3-0*, Chairman's Remarks on cover insert.
[56] Joint Chiefs of Staff, JP 3-13, II-2.
[57] Ibid., III-1.
[58] James O Ellis, *View from the Top* (Briefing Slides on Power Point Presentation), page 17.
[59] Ibid.,16.
[60] Ibid.,19.
[61] Joint Chiefs of Staff. *JP 3-0*, III-9.
[62] Ibid., III-10.
[63] Ibid., III-11.
[64] Joint Chiefs of Staff. *JP 3-13*.
[65] Ibid.
[66] This area requires closer study. In the author's opinion, a great deal of effort and resources has been dedicated to the affects of peer and near-peer technologies and "what-if" scenarios but little has been accomplished to capture low-tech conflict during the 1990s, determine the lessons learned and apply them to the joint informational doctrinal process.
[67] Joint Chiefs of Staff. *JP 3-13*, I-1.
[68] Ibid., I-2.
[69] Joint Chiefs of Staff. *JP 3-0*, III-12.
[70] Joint Chiefs of Staff. *JP 0-2*, IV-11.
[71] Joint Chiefs of Staff. JP 3-0, Insert Cover.

BIBLIOGRAPHY:

Articles

Barwinczak, Patricia M. "Achieving Information Superiority" *Military Review* (September - November 1998): 36 – 43.

Bass, Carla D. "Building Castles on Sand: Understanding the Tide of Information Operations" *Airpower Journal* (Summer 1999): 27 – 45.

Bellamy, Chris. *The Future of Land Warfare*. New York: St. Martin's Press, 1987.

Bunker, Robert J. "Information Operations and the Conduct of Land Warfare" *Military Review* (September - November 1998): 45 - 53.

Church, William. "Kosovo and the Future of Information Operations". Center for Infrastructure Warfare Studies. Database on-line. Available at www.Iwar.org.

Clausewitz, Carl von. *On War*. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

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

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

Books

Allard, Kenneth. *Somalia Operations: Lessons Learned*. Washington, DC: National Defense University Press, 1995.

Friedman, George and Meredith. *The Future of War.* New York: St. Martin's Griffin, 1998.

Leonhard, Robert R. *The Principles of War for the Information Age.* Novato: Presido Press, 1998.

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

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

Pillsbury, Michael. ed. *Chinese Views of Future Warfare*. Washington DC: National Defense University Press, 1997.

Stein, Jess. ed. *Random House Dictionary, College Edition*. New York: Random House Inc., 1975.

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

Van Creveld, Martin. *Technology and War*. New York: Free Press, 1989.

_____. *The Transformation of War*. New York: Free Press, 1991.

Waltz, Edward. *Information Warfare: Principles and Operations*. Norwood, Artech House, 1998.

Primary Resources

Ellis, James O. *A View from the Top.* Briefing presented as part of the After Action Review on Task Force Noble Anvil.

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

_____. *Joint Vision 2010.* Washington, DC: Government Printing Office, 1996.

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

_____. *Joint Publication 1-01: Joint Publication System*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 1-01.1: Compendium of Joint Publications*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 1-02: Department of Defense Dictionary and Associated Terms*. Washington, DC: Government Printing Office, 1999.

_____. *Joint Publication 2-02: National Intelligence Support to Joint Operations*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 3-0: Doctrine for Joint Operations*. Washington, DC: Government Printing Office, 1995.

_____. *Joint Publication 3-03: Doctrine for Joint Interdiction Operations.*

Washington, DC: Government Printing Office, 1997.

_____. *Joint Publication 3-05: Doctrine for Joint Special Operations*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 3-09: Doctrine for Joint Fire Support*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 3-13: Joint Doctrine for Information Operations*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 3-13.1: Joint Doctrine for C2W*. Washington, DC: Government Printing Office, 1998.

_____. *Joint Publication 3-33: Joint Force Capabilities*. Washington, DC: Government Printing Office, 1999.

_____. *Joint Publication 3-53: Doctrine for Joint Psychological Operations*. Washington, DC: Government Printing Office, 1996.

_____. *Joint Publication 3-54: Joint Doctrine for Operations Security*. Washington, DC: Government Printing Office, 1997.

_____. *Joint Publication 3-57: Doctrine for Joint Civil Affairs*. Washington, DC: Government Printing Office, 1995.

_____. *Joint Publication 3-58: Joint Doctrine for Military Deception*. Washington, DC: Government Printing Office, 1996.

_____. *Joint Publication 3-61: Doctrine for Public Affairs in Joint Operations*. Washington, DC: Government Printing Office, 1998.

_____. *Memorandum on Implementation Policy for Joint Vision 2010*. CJCSI 3010.01, dated 10 Oct 1997. Database on-line. Available at Joint Electronic Library, 1997.

_____. *National Military Strategy of the United States*. Washington, DC: Government Printing Office, 1997.

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

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

_____. *Air Force Vision Statement*. Washington DC: Department of the Air

Force, 1997.

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

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

_____. *Draft Field Manual 100-6, Information Operations*. Fort Leavenworth: Center for Army Doctrine, 1999.

_____. *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*. Washington DC: Government Printing Office, 1994.

US Marine Corps. *Operational Maneuver from the Sea: A Concept for the Projection of Naval Power Ashore*. Washington DC: United States Marine Corps, 1997.

_____. *A Concept for Information Operations*. Quantico: Marine Corps Combat Development Command, 1998.

US Navy. *Forward from the Sea*. Washington DC: Department of the Navy, 1997.

_____. *Naval Doctrine Publication 6: Naval Command and Control*. Washington DC: Department of the Navy, 1995.

US Special Operations Command. *Special Operations Reference Manual*. Washington DC: Special Operations Command, 1998.

Theses

Dick, Sameul R. "The Operation Proponent for Information Warfare". Master's Thesis, Naval War College, 1998.

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

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

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

Jensen, William J. "Information Warfare's Missing Quarterback: The Case for a

Joint Force Information Warfare Component Commander". Master's Thesis, Naval War College, 1998.

Marr, Patrick M. "Information Warfare and the Operational Art". Master's Thesis, Naval War College, 1996.

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

Schifferle, Peter J. "Incorporating Enemy Psychological Vulnerability into US Army Heavy Division IPB Doctrine". Master's Thesis, School of Advanced Military Studies, Fort Leavenworth, 1993.