CMSA Technical Report: 97-04
A VALUE FUNCTION APPROACH TO INFORMATION OPERATIONS MOE'S: A PRELIMINARY STUDY

WORKING PAPER SERIES

CENTER FOR MODELING, SIMULATION, AND ANALYSIS
DEPARTMENT OF OPERATIONAL SCIENCES

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

SCHOOL OF ENGINEERING
Wright-Patterson Air Force Base, Ohio

DISCLAIMER

The opinions stated in this document are solely those of the authors and do not reflect the official policy or positions of the Environmental Protection Agency, the Department of Energy, Department of Defense, or the U.S. Government.

CMSATR/97-04

CENTER FOR MODELING, SIMULATION, AND ANALYSIS
TECHNICAL REPORT 97-04

Center for Modeling, Simulation, and Analysis

Department of Operational Sciences

Air Force Institute of Technology

Air University, Air Education and Training Command, USAF

Authors: Capt Michael P. Doyle, USAF; Dr. Richard F. Deckro;
Lt Col Jack A. Jackson Jr., USAF; LTC Jack M. Kloeber Jr., USA

A VALUE FUNCTION APPROACH TO INFORMATION OPERATIONS MOE'S: A PRELIMINARY STUDY

JULY, 1997

ABSTRACT

A value-focused thinking approach is applied to information operations. A preliminary value hierarchy for information operations is constructed by extracting the values of senior military leadership from existing doctrine. To identify these key values for information operations, applicable existing doctrine was reviewed and summarized. Additionally, hierarchical representations of the values represented within each reviewed doctrine are developed.

A value hierarchy requires that supporting objectives be mutually exclusive and collectively exhaustive. Within this analysis, these requirements are enforced, in part, by developed definitions which serve as tests to maintain mutual exclusivity. An exhaustive set of supporting values is also guaranteed by identifying a spanning set of values that directly support the overall objective of information operations.

This preliminary value hierarchy serves as the basis for continuing research. The implications for this research include the construction of a prescriptive model in which the effectiveness of current and future systems can be assessed on a common scale. Further, the effectiveness of developing technologies can be assessed and the value of these technologies determined with respect to the values of senior military leadership. With this, the value of "holes" in our suite of information warfare systems can also be assessed in terms of their effectiveness in fulfilling the values of military leadership.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

I. Introduction

With the recent passage from the industrial age to the information age, a great deal of attention has been focused on exploiting the newly defined "information realm" with ever-advancing technological capabilities. The weapons for conducting operations against information and information systems (information operations) are growing in number and capability. Globally interconnected telecommunications and computing systems alter perceptions of engagement by providing direct connectivity between adversaries despite disparate locations. Distances that are considered vast by air, land, and sea forces are considered negligible by information operators who are exploiting direct connectivity half a world away. In contrast, distances too small to be considered by air, land, and sea forces are seen as infinite by an information operator that cannot access a system whose modem connector has come ajar. With this connectivity, access is obtained to the information flows and stores upon which our nation is growing increasingly dependent. When this information is employed in the decision making processes that affect national priorities, objectives, or defense, access is then provided to the decision making processes; knowingly or unknowingly.

Master Sun recognized in 500 BC that the mind of the enemy is the primary target of the skilled general [Griffith, 1971: 41]. Throughout military history, this imperative has been continually restated and reaffirmed by masters of strategy; from the ancient commentaries of Ho Yen-Si to the writings of Niccolo Machiavelli through this century and the works of Mao Tse-tung and others focusing on a foe's hearts and minds. This imperative, however, is even more meaningful today as global connectivity links potential adversaries, ranging from aggressor regimes or simply disgruntled individuals.

> *"All warfare is based on deception. A skilled general must be a master of the complementary arts of simulation and dissimulation: while creating shapes to confuse and delude the enemy he conceals his true dispositions and ultimate intent. When capable he feigns incapacity: when near he makes it appear that he is far away: when far away that he is near. Moving as intangibly as a ghost in the starlight, he is obscure, inaudible. His primary target is the mind of the opposing commander: the victorious situation, a product of his creative imagination."*
>
> *Sun Tzu*

The technological capability and information dependency of the United States opens the door to exploitation by hostile agents who, more than likely, do not share similar informational and technological vulnerabilities; creating a broad asymmetry in technological capability and dependency. The means and

methods of defense against this form of attack are, therefore, of the foremost priority.

Offensively, the ability to conduct a full range of operations in the information realm, shaping and exploiting the battlespace, is critical to achieving national objectives. New weapons and tactics are being developed as we form information operations centers throughout the Department of Defense and as a new Battlelab stands up.

With this, being the dawn of a new activity, accepted and robust measures of merit (MOMs) that represent the ability of a weapon system to meet the objectives of information operations have yet to be established. Without these acceptable measures of merit for information weapons, it is a much more difficult problem to plan or model their use. Further, if the full value of such weapons can not be completely communicated, these systems may not be developed, acquired, or deployed appropriately to support joint operations and defend national interests.

Unlike traditional MOMs for "hard kill" weapons that focus on the single attribute of lethality, systems employed by information operators require multiple attributes to represent the weapon's characteristics and effectiveness. These key characteristics that information operations weapons bring to our national arsenal and command structure can provide an initial framework by which to consider MOMs for information operations weapons. A means of assessing these key characteristics (attributes) in terms of the objectives of information operations is value focused-thinking.

Value-focused thinking (VFT) is used in this study to assign value to weapon systems based on the ability (merit) of these systems to accomplish the objectives set forth by national-level decisionmakers. The primary reason for applying VFT is to establish quantifiable and understandable means of assessing the measures of merit of narrow classes of information operations systems. From existing value models that represent the values held by stake-holding decisionmakers, a hierarchy of objectives, functions, and operational tasks for information operations is constructed which reflects the joint commander's values. By matching the force qualities of weapon systems to the objectives of the information operations, weapon systems are assessed in terms of their ability to meet desired objectives. Matching these measures of merit to the attributes of near-term and currently available systems provides a means for assessing prescriptively the merit of information operations weapons systems and weapons technologies both current and future using a common scale, scored by experts against the objectives of decisionmakers.

II. Measures of Merit: Methodology

The definition and interpretation of measures of merit (MOM) has evolved to meet the needs of decisionmakers and the changing nature of warfare. Faced with the need to evaluate multi-attribute alternatives for incorporation into complex systems, decisionmakers need more information than a single-valued measure of merit can provide. Difficulties are encountered when trying to develop single-valued MOMs for assessing complex systems. These difficulties stem from an attempt to assess subjective attributes of systems that do not translate well into a uniquely quantifiable single measure. The limitations of using single-valued MOMs to assess a system of systems, then, follow from the "apples" and "oranges" of the quantified multiple attributes that represent the merit of a system in a given application [Pinker, 1995: 8-12]. Broader, multiattribute, MOMs are less certain than the traditional single-valued quantities like system range or muzzle-velocity, but the sophistication of the measures permits a broader perspective and provides the decisionmaker with information necessary to make better decisions.

Making and acting on good decisions are the keys to success. The factors that enter into making a decision are the properties that represent each aspect of the decision making process; the measures of merit of competing alternatives from the perspective of the decisionmaker. These measures of merit represent what is favorable or unfavorable about an alternative in a particular decision context, expressed in terms of the decisionmaker's values.

What is unusual about developing MOMs for information operations is that the field of information is relatively new and continually developing. The tools employed are changing at least as rapidly. Any means of assessing merit based on existing alternatives is therefore likely to be outdated faster than the technology it is assessing. Because of this a prescriptive, rather than descriptive, means of assessing value is needed. Value-focused thinking is also an excellent option for this type of analysis.

II.1. Value-Focused Thinking

VFT starts with the decisionmaker's values [Keeney, 1992]. These values are represented by a hierarchy of objectives. The overarching objective is the strategic objective. The most important values supporting the attainment of the strategic objective are represented by fundamental objectives. Fundamental objectives are accomplished by means objectives. In general, higher-tier objectives are decomposed until a set of

measurable, understandable, and operational attributes are developed that measure the degree to which the higher-tier objective is fulfilled [Keeney, 1992: 192]. These quantifiable, understandable, and operational attributes then serve as the measures of merit for the systems applied to the decision context.

In his book, Value Focused Thinking: A Path to Creative Decisionmaking, Keeney defines two types of decision situations; decision problems and decision opportunities [Keeney, 1992: 49]. Decision problems are faced when the decisionmaker must choose from existing alternatives to solve the problem at hand. Decision opportunities are best described as situations in which the decisionmaker has the ability to generate alternatives before selecting from all alternatives [Keeney, 1992: 9]. Because decision opportunities concentrate on choosing better alternatives, the decisions made can be superior to the incremental tweaking that comes from starting with only the existing alternatives. Table 1 compares the processes involved with alternative-focused and value-focused thinking in both decision problem and decision opportunity applications as described by Keeney [Keeney, 1992: 49]. The scope of this table has been limited to the case in which the strategic objective has been set.[1]

Table 1: Alternative-Based Thinking Vs Value-Focused Thinking[2]

Step	Alternative-Focused Thinking Decision Problems	Value-Focused Thinking Decision Problems	Value-Focused Thinking Decision Opportunities
1	Recognize decision problem	Recognize decision problem	Specify values
2	Identify alternatives	Specify values	Create a decision opportunity
3	Specify values	Create alternatives	Create alternatives
4	Evaluate alternatives	Evaluate alternatives	Evaluate alternatives
5	Select an alternative	Select an alternative	Select an alternative

The intent is to apply VFT to the decision opportunity of MOMs for information warfare (IW) systems. The obvious conflict is that many of the systems applicable to information operations (IO) already exist and furthermore; only existing systems may be applied operationally. This appears to make a case for alternative-focused thinking (descriptive analysis) which would generate a useful and important decision making tool that is limited in scope to existing systems in a descriptive fashion. In alternative focused thinking, however, viable (perhaps better) alternatives are often missed, fundamental objectives can be unfulfilled by the decisions developed to meet lower-tier objectives that do not meet the higher-tier objectives (providing a means to decision consequences and not the objectives), and alternatives and objectives are not necessarily logically matched [Keeney, 1992: 44].

---

[1] The difference is that without a strategic objective, the first step is to identify a decision opportunity, then specify values.

[2] Keeney, Ralph L., Value Focused Thinking: A Path to Creative Decisionmaking, (Cambridge, Mass.: Harvard University Press, 1992), p. 49.

Developing MOMs for a decision opportunity with a value-focused perspective (prescriptive analysis) permits assessment of systems before, during, and after development; provides a means to identify operational needs not being met with current and near-term developmental systems; and provides a framework that represents the values of military leadership from which to assess application and implementation of systems and tactics.

Military applications of VFT that are prescriptive in nature include Spacecast 2020 and Air Force 2025. The results of these studies confirm that VFT is a superior means of assessing rapidly developing decision opportunities by developing a common framework by which current and future systems may be evaluated. The context, perspective, and methodology of VFT is assessed to be a superior methodology for the purpose of constructing a prescriptive value-based means of assessing the merit of current and future weapon systems on a common scale that represents the objectives set forth by national-level decisionmakers. Because of this, VFT is chosen as the means of addressing this decision opportunity. To properly apply this methodology, the decision frame, its context and strategic objective, must first be defined.

III. Framing the Decision

A decision is framed by integrating the decisionmaker's values and the available alternatives [Keeney, 1992: 30]. This is accomplished by defining the decision context (alternatives available) and the fundamental objectives (values) of the decisionmaker. The available alternatives are considered to reside in an alternative space that contains all feasible alternatives, both present and future. This set of all feasible alternatives is then limited by the values of the decisionmaker, termed a decision frame. A conceptual decision frame is shown in Figure 1.[3]

The decision context bounds the alternative space; that set of alternatives that are appropriate for a specific situation [Keeney, 1992: 30]. The decision context should, therefore, be as wide as possible since any artificially small alternative space will limit the alternatives available to the decisionmaker both in the present and into the future. To completely frame a set of all possible alternatives, however, the strategic objectives of the decisionmakers are required.

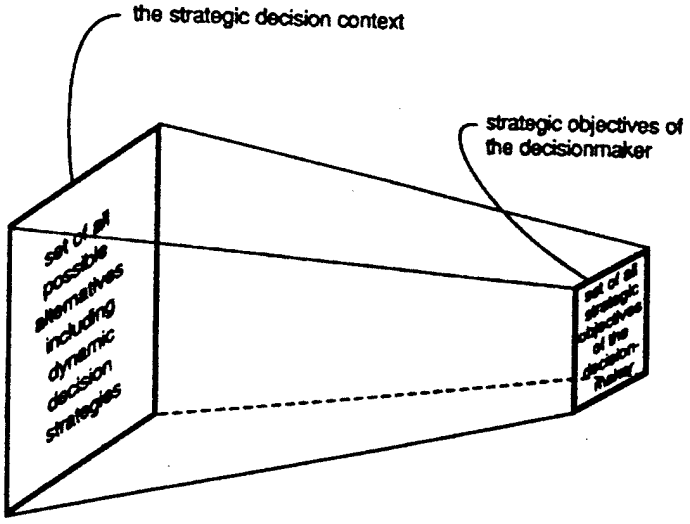

Figure 1:The Strategic Decision Frame Facing a Decision Maker[4]

Strategic objectives are intended to guide all decision making within the given context [Keeney, 1992: 41]. Strategic objectives are decomposable into fundamental objectives, these fundamental objectives are further decomposed into means objectives, and so forth until a set of understandable, quantifiable, and operational set of attributes are extracted. These attributes are the means of assigning values to the measures of merit of IO weapon systems. This is represented by Keeney in Figure 2. By exploiting this decomposition, a hierarchical set of objectives is developed that collectively fulfill the strategic objective.

---

[3] This representation projects the values of the decisionmaker onto the decision context. The alternatives that satisfy both the values and the decision frame are then circumscribed by the decision frame.

[4] Keeney, Ralph L., "Value Focused Thinking: A Path to Creative Decision-Making," (Cambridge. Mass.: Harvard University Press, 1992), pp. 41.

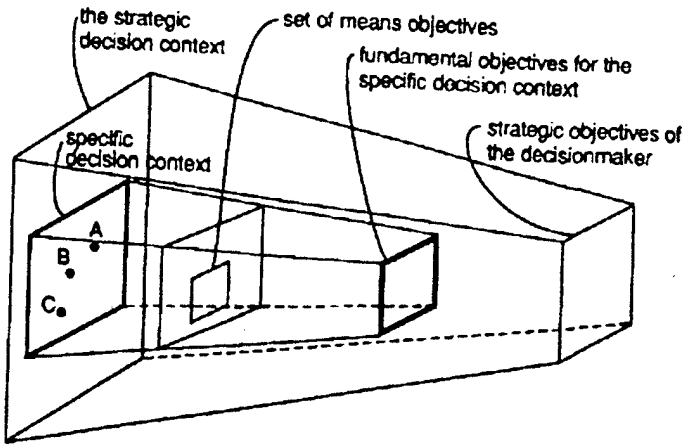

Figure 2: Hierarchical Decision Frame[5]

[5] Keeney, Ralph L., "Value Focused Thinking: A Path to Creative Decision-Making," (Cambridge, Mass.: Harvard University Press, 1992), pp. 45.

IV. Fundamental Objectives

Fundamental objectives are the means to attain the strategic objectives. To fulfill the strategic objective, fundamental objectives must span the decision context, limited only by the strategic objective (which means that the fundamental objectives should be collectively exhaustive). To enable decomposition into a useful set of measurable, understandable, and operational attributes, all fundamental objectives should be mutually exclusive of each other (nonredundant). The requirement of mutual exclusivity is easily understood by viewing the objectives that support the fundamental objectives; these are termed means objectives. If a means objective is to support the fundamental objective, and the fundamental objective to support the strategic objective, any failing of mutual exclusivity will cause the lower-tier objective to be assessed as more effective at accomplishing the strategic objective than is warranted by its true merit; this is termed double counting. Double counting then skews the measures of merit, yielding a false assessment of effectiveness for all evaluated systems.

Table 2: Desired Properties of the Set of Fundamental Objectives[6]

	Fundamental Objectives Should Be:
1	*Essential* - To indicate consequences in terms of the fundamental reasons for interest in the decision situation
2	*Controllable* - To address consequences that are influenced only by the choice of alternatives in the decision context
3	*Complete* - To include all fundamental aspects of the consequences of the decision alternatives
4	*Measurable* - To define objectives precisely and to specify the degrees to which objectives may be achieved
5	*Operational* - To render the collection of information required for an analysis reasonable considering the time and effort available
6	*Decomposable* - To allow the separate treatment of different objectives in the analysis
7	*Nonredundant* - To avoid double-counting of possible consequences
8	*Concise* - To reduce the number of objectives needed for the analysis of a decision
9	*Understandable* - To facilitate generation and communication of insights for guiding the decision making process

[6] Keeney, Ralph L., "Value Focused Thinking: A Path to Creative Decision-Making," (Cambridge, Mass.: Harvard University Press, 1992), pp. 82.

The relationship between objectives at different tiers represents a fundamental objectives hierarchy. In this hierarchy, Keeney defines the lower-tier objectives as those that answer, "what aspects of the higher-tier objective are important," [Keeney, 1992: 71]. This applies to the fundamental objectives as they define and delimit the strategic objective as well as to the means objectives that define and delimit the fundamental objectives.

Keeney's definitions of the desirable properties of fundamental objectives, shown in Table 2. Along with this list, Keeney points out that multiple fundamental objectives hierarchies can be created for the same decision problem, but some hierarchies are better than others based upon such criteria as measurability, understandability, or operability, as highlighted in Table 2. The formation of the hierarchy is a creative process that relies on the judgments of decisionmakers and knowledgeable agents, which implicitly means that hierarchies for any decision are not necessarily unique.

V. Building a Hierarchy

Structuring fundamental objectives into a hierarchy provides insight into the values that are important in the context of the decision. The hierarchy also aids and improves the quality of analysis stemming from the application of value focused thinking to a decision opportunity. Keeney sites the advantages of using a value hierarchy in order to specify the important values that guide the decision making process. These advantages are shown in Table 3.

Table 3: Advantages of Structuring Fundamental Objectives Into a Value Hierarchy[7]

	Advantages of Structuring Fundamental Objectives
1	The higher levels of an objectives hierarchy relate to fairly general concerns...consequentially, they can be identified relatively easily
2	Higher-level objectives provide a basis for specification of lower-level objectives
3	A hierarchy helps identify missing objectives, since logical concepts of the specification process can easily identify holes in the hierarchy
4	The distinctions between means objectives and fundamental objectives become clearer as the objectives hierarchy is structured
5	Situations where redundancy or double-counting might occur can often be identified with the logic of an objectives hierarchy
6	It is easier to identify attributes to measure the achievement of more specific (lower-level) attributes than of more general (higher-level) objectives
7	The attributes for lower-level objectives collectively indicate the degree to which the associated higher-level objective is achieved
8	The complete set of lowest-level attributes for a fundamental objectives hierarchy provides a basis for describing the consequences in the decision problem and for asserting an objective function appropriate for the problem

The development of a hierarchy requires identification and structuring of objectives. Identification requires assessing values—but whose values? The values of the top-level decisionmaker appropriate to the decision context are sought because, presumably, these represent the overall values of the organization—ones accepted by all involved. Finding this "gold standard" greatly simplifies the creation and proper structuring of a hierarchy [Parnell et al., 1997].

[7] Keeney, Ralph L., "Value Focused Thinking: A Path to Creative Decision-Making," (Cambridge, Mass.: Harvard University Press, 1992), pp. 86-87.

We can have strategic, fundamental, and means objectives as the basic elements of any hierarchy. The appropriate structuring of these objectives is critical to developing a useful hierarchy. Each lower-tier objective must narrow the decision context to an increasing level of resolution if a quantifiable attribute is to be obtained. This is represented in Figure 3. This, then, provides a requirement and, therefore, a means of testing precedence in objective structuring. With this understanding, the values and objectives of senior leadership are sought, decomposed and formed into a hierarchy.

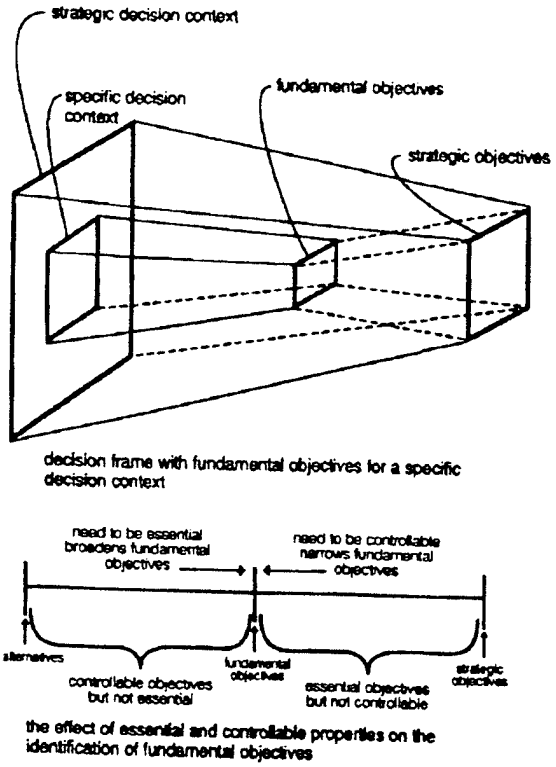

Figure 3: Identifying and Structuring Objectives[8]

[8] Keeney, Ralph L., "Value Focused Thinking: A Path to Creative Decision-Making," (Cambridge, Mass.: Harvard University Press, 1992), pp. 84.

VI. Locating a Gold Standard

To locate acceptable objectives, both strategic and fundamental, from which to form an initial decision frame for information warfare, military doctrine was reviewed. In this, the most recently available doctrinal papers regarding information warfare were reviewed. Included in this review are joint doctrines that support key requirements of information warfare. In order to keep the decision context as broad as possible, the doctrinal papers were applied in a preferential order in which joint doctrine was preferred, service specific, and agency specific papers were then used to make as complete a model as possible.[9]

Doctrine exists for virtually all areas of military operations. Doctrine sets the standards and requirements for all military operations. The most overarching of these is JV 2010. At the Air Force level, Global Engagement is the most recent doctrinal publication, preceded by Global Presence, and Air Force Manual 1-1. These publications establish the requirements of Information Warfare acting in support of established doctrine. These roles for Information Warfare are descriptive in nature describing the functions of information operations in support of the joint and Air Force objectives.

Joint doctrine is, itself, hierarchically structured as shown in Figure 4. Within this structure, the Joint Publication 3-series for joint operations was selected as the most appropriate for initial analysis. The structure of the 3-series Joint Publications is shown in Figure 5.

[9] It could be argued that the commercial and private sectors should be considered from a broad national doctrine that spans the politico-military, corporate, and civil sectors. This is beyond the span of control of the military though these sectors might be partially addressed as part of the military's span of influence.

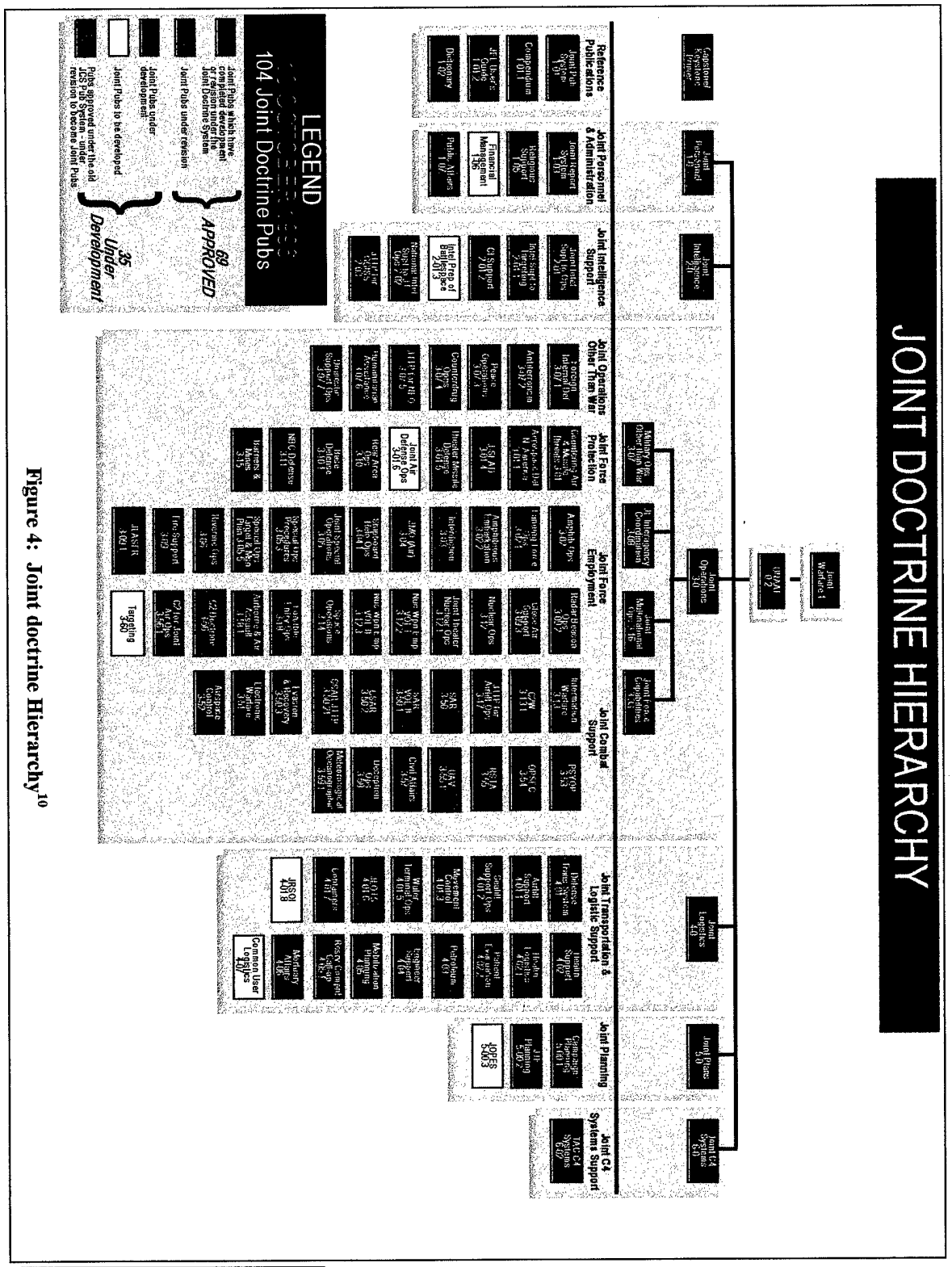

Figure 4: Joint doctrine Hierarchy[10]

[10] Joint Doctrine from Defense Technical Information Center: http://www.dtic.mil/doctrine/docinfo/pstatus/hierchart.htm, 28 Feb 1997.

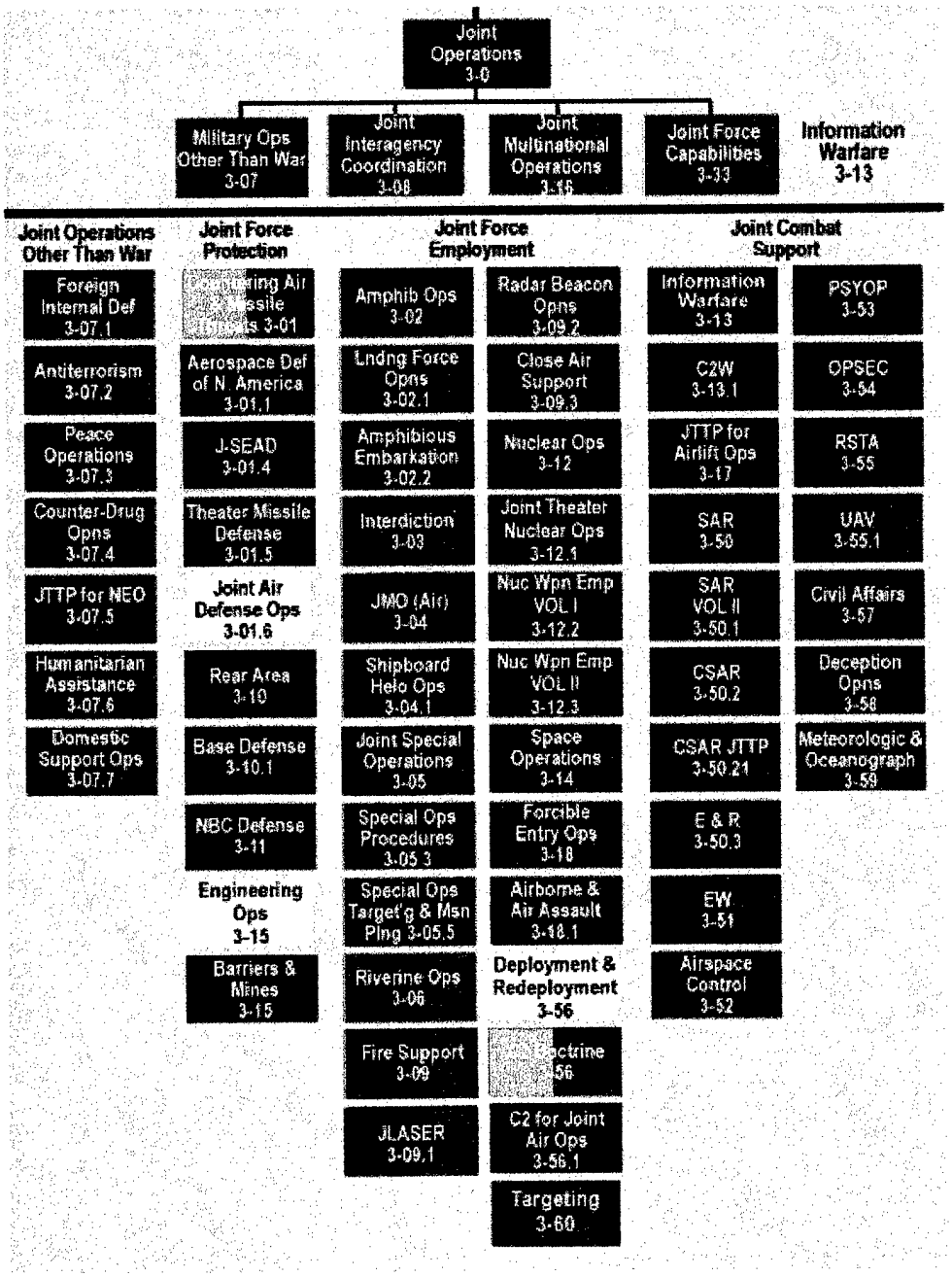

Figure 5: Joint Publications regarding Joint Operations[11]

[11] Joint doctrine Hierarchy from Defense Technical Information Center: http://www.dtic.mil/doctrine/docinfo/pstatus/hierchart.htm, 28 Feb 1997.

VI.1. Joint Vision 2010

Joint Vision 2010 (JV 2010) defines four new operational concepts—Dominant Maneuver, Precision Engagement, Focused Logistics, and Full-Dimensional Protection; that serve as a set of objectives for all future military operations. These four concepts serve as the fundamental objectives in support of the key characteristic sought for our military forces in the 21st Century—Full Spectrum Dominance [JV 2010: 2]. Each operational concept that makes up the "framework" of Full-Spectrum Dominance requires information superiority. This is explicit in Figure 6 and in the following statement from JV 2010: "The basis for this framework is found in the improved command, control, and intelligence which can be assured by information superiority," [JV 2010: 19]. The need for information superiority in each of JV 2010's "fundamental objectives" causes information superiority to be redundant in this model. JV 2010, therefore, fails to establish an adequate value model for assessing information operations.

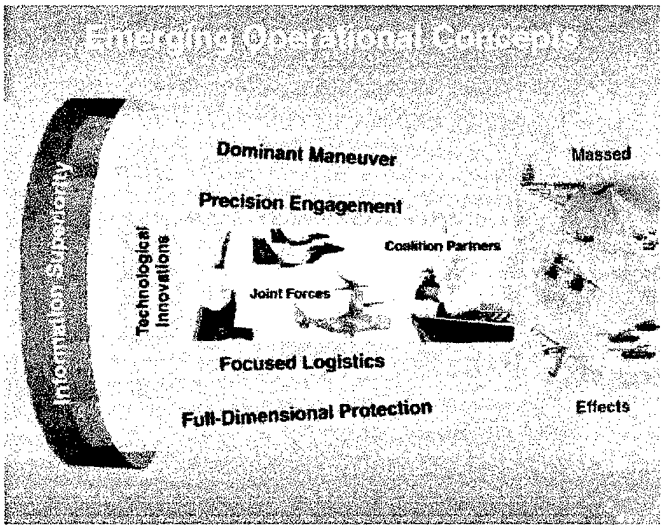

Figure 6: Joint Vision's Reliance on Information Superiority[12]

JV 2010 does, however, reflect the values of the top military leadership. These values are extracted and employed to start model construction. Highlighted in JV 2010 is the "imperative of jointness." Jointness highlights reduced redundancy, reduced costs while retaining effectiveness, and more seamless integration [JV 2010: 8]. To achieve this, the services "must be fully joint: institutionally, organizationally, and technically," [JV 2010: 9]. Emerging technology and improved capabilities are recognized as having an enormous impact on military forces in the near future. Increased precision, broader ranges of weapons effects, advances in low-observable technologies, an improvements in information and systems integration technologies are all anticipated to significantly impact future military operations [Joint vision 2010: 11-13].

[12] Joint Vision 2010, OPR, chairman of the Joint Chiefs of Staff, Pentagon, Washington, DC 20318-5126, p. 19.

Returning to information specific elements of JV 2010, information and systems integration technologies are expected to provide decisionmakers with accurate information in a timely manner. Increased information technologies are expected to improve the ability to see, prioritize, assign, and assess information. The criticality of complete joint integration of information and information systems is highlighted in JV 2010 by the following; "The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistics support centers will allow a greater number of operational tasks to be accomplished faster," [Joint vision 2010: 13]. Increased tempo with smaller, more-lethal forces will be able to exploit increased computing capabilities, global positioning, and telecommunications; gaining dominant battlespace awareness.

JV 2010 defines dominant battlespace awareness as an interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest. While this is not expected to eliminate the fog of war, it will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it [JV 2010: 13].

In JV 2010, the age old reliance of all military operations on information superiority is recognized, but so too are the rapid and revolutionary advances in information collection, processing, and dissemination (Figure 7). With this revolution in military affairs, the influence of information drives the need for information superiority. JV 2010 defines information superiority as *"the capability to collect, process, and disseminate and uninterrupted flow of information while exploiting or denying an adversary's ability to do the same"* [JV 2010: 16]. Additionally, information superiority as defined in JV 2010 necessarily has offensive and defensive components. Offensive information warfare degrades or

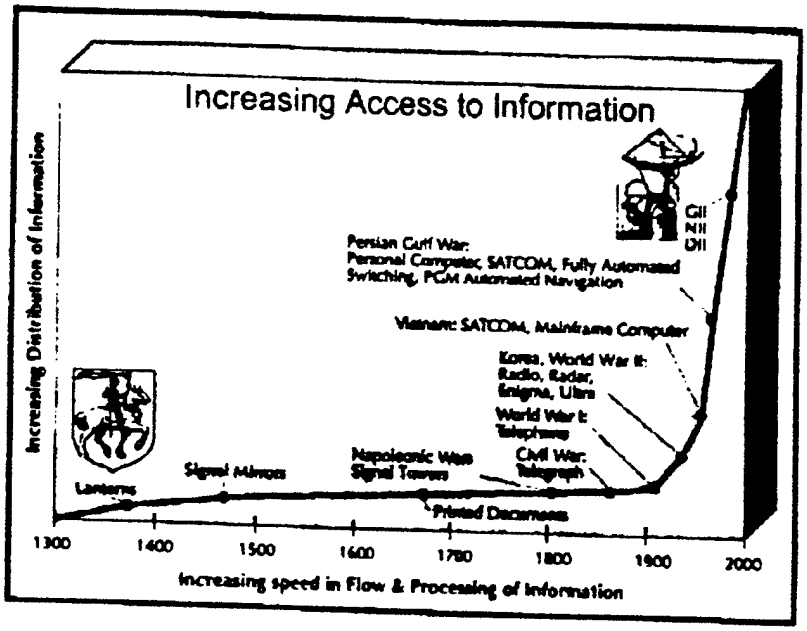

Figure 7: The Rise of Information Access[13]

[13] Joint Publication 3-13 (First Draft) 21 Jan 1997, p. I-21.

exploits an adversary's collection or use of information, while defensive information warfare protects the ability to conduct information operations [JV 2010: 16]. While no hierarchy is offered in JV 2010, one is extracted from the objectives, values, and components expressed in the text (see Figure 8).

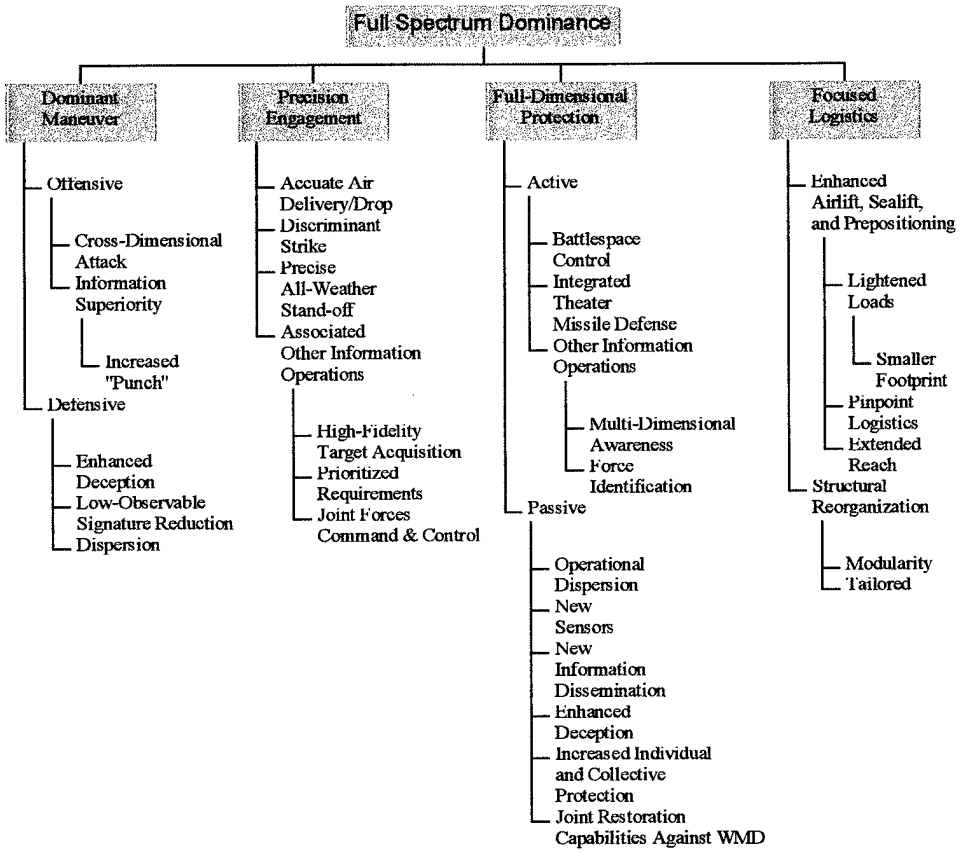

Figure 8: Extracted Functional Hierarchy from Joint Vision 2010

By extracting value statements from JV 2010, a fundamental hierarchy for information superiority is constructed that represents the leaderships' thoughts on the future of information operations (Figure 9).

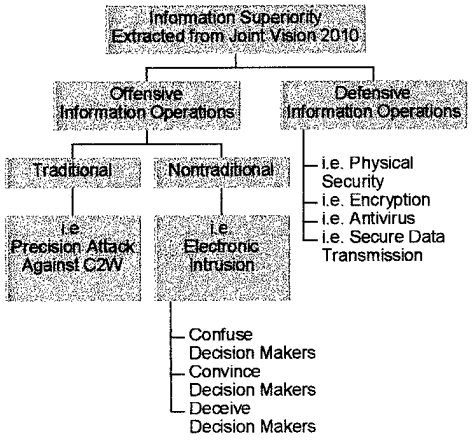

Figure 9: Information Superiority Hierarchy From Joint Vision 2010

VI.2. Cornerstones of Information Warfare

The earliest Air Force specific contributions to IW reviewed for this analysis is titled Cornerstones of Information Warfare (1995) [Widnall]. This paper helped set the course for the IW papers that followed both in concept and definition. In this paper, information is defined as a separate realm--distinct from air, land, sea, and space [Widnall: 2]. The definitions surrounding information warfare were formalized and presented in an operational context. These definitions are shown in Figure 10.

Definitions from the Cornerstones of Information Warfare

Counterinformation - Actions dedicate to controlling the information realm.

Defensive Counterinformation - Actions protecting our military information functions.

Direct Information Warfare - Changing the adversary's information without involving the intervening perceptive and analytical functions.

Indirect Information Warfare - Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Information - Data and instructions.

Information Attack - Directly corrupting information without visibly changing the physical entity within which it resides.

Information Function - Any activity involving the acquisition, transmission, storage, or transformation of information.

Information Operations - Any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces.

Information Warfare - Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions.

Military Information Function - Any information function supporting and enhancing the employment of military forces.

Offensive Counterinformation - Actions against the adversary's information functions.

Figure 10: Terminology from the 1995 Publication, "Cornerstones of Information Warfare[14]

Cornerstones also identified the functions that support counterinformation; both offensive and defensive. Traditional means of conducting information warfare are those elements of command and control warfare (C2W); psychological operations, electronic warfare, military deception, physical destruction, and various security measures. These measures can be integrated and applied in order to; *control* the information realm, *exploit* our control of information, *enhance* our overall force effectiveness [Widnall: 9]. This document served as a pathfinder for entry into information operations, and provided a hierarchy of functions that reflects the decisionmaker's values. A refined hierarchy is developed that is consistent with the hierarchies extracted

from all other IO related doctrines (see Figure 11). This hierarchy includes the traditional functions of command and control warfare (C2W) and the new functions of the larger set of information operations.

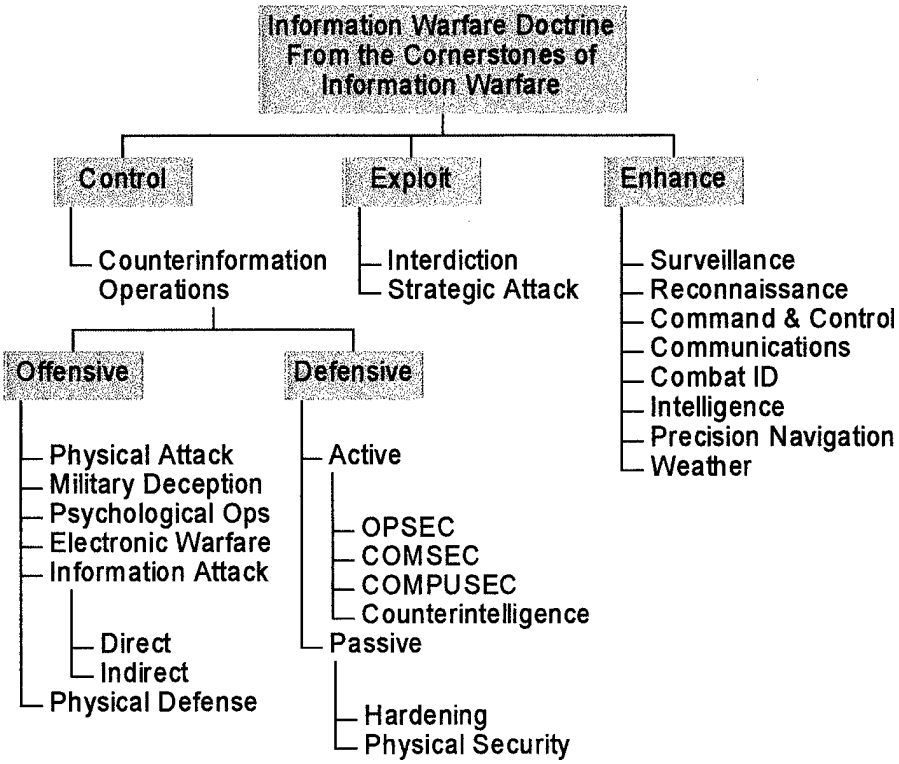

Figure 11: Extracted Information Warfare Doctrine from the Cornerstones of Information Warfare

This hierarchy is of limited utility as a fundamental objectives hierarchy, but serves as a point of discussion. The three objectives of control, enhance, and exploit are extracted elements from existing air power doctrine. These capture the intent of information warfare, and are mutually exclusive but not necessarily collectively exhaustive in meeting the strategic objective of acquiring, exploiting, and protecting information in support of national objectives [Widnall: 3]. The reason Cornerstones is assessed as not collectively exhaustive for the purposes of this analysis is that it was framed as a service specific paper and as such has been superseded both within and outside of the Air Force.

[14] Widnall, Sheila, E., Fogleman, Ronald R., "Cornerstones of Information Warfare," pp.13-14.

VI.3. AF/IN White Paper

The framework established at the Air Force level by the Cornerstones of Information Warfare appears to be reflected in another important document—the AF/IN White Paper titled Air Force Intelligence and Information Warfare [Abraham, 1996]. This paper established the Intelligence community's expectation of its role in information warfare. The AF/IN White Paper was more prescriptive in nature than the Cornerstones of Information Warfare, clearly defining the bounds of the *information realm.*

In this paper, intelligence support was focused with the intent of directly influencing the information realm by both direct and indirect means [Abraham, 1996: 3]. Intelligence functions, as part of the larger set of information functions, were considered a means of impacting the struggle for information dominance—defined as the primary objective of IW. The terms defined in the AF/IN White Paper are presented in Figure 12. Using this terminology, a specific hierarchy is developed for IW as shown in Figure 13.

Terminology used in the AF/IN White Paper

Information Warfare - Any action to deny, exploit, corrupt, or destroy the enemy's information and its functions, protecting ourselves against those actions; and exploiting our enemy's own military information functions.

Information Dominance - A primary objective of IW. It is the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same. ID includes gaining control over the information realm (information superiority) and fully exploiting military information functions.

Information Realm - Information is a realm, just like air space, land, and sea. Like all realms, military's seek to dominate it. It is composed of three elements: information, information systems, and information functions.

Information - Data and the instructions required to give the data meaning.

Information System - Any physical component used to acquire, transmit, store, or transform information (i.e. people, wires fibers, telephones, radar).

Indirect IW - Relies on the adversary's ability to gather and process data. This refers to actions against the information processor, not the information itself. Degrading, destroying, or manipulating information processing ranging from perception management (PSYOP) to technical management (deception to EW).

Direct IW - Affecting the enemy's information itself.

Counterinformation - Activities dedicated to controlling information, maintaining access to information, and securing the integrity of one's own information, while denying or disrupting the adversary's access to information. Attaining and maintaining control over the information realm can be achieved through a combination of offensive counter information (OCI) and defensive counter information (DCI).

Mapping the Battlespace - Real-time awareness of the location, status, and intentions of the adversary, established by penetrating his virtual landscape to include communications networks, nodes, computer technology, and cognitive interaction.

Shaping the Battlespace - Constraining and channeling the enemy into a spiraling path of exploitation. To manipulate the enemy to the point where minor applications of physically destructive force have maximum effect and the risk to US forces is minimized.

Figure 12: AF/IN White Paper Terminology

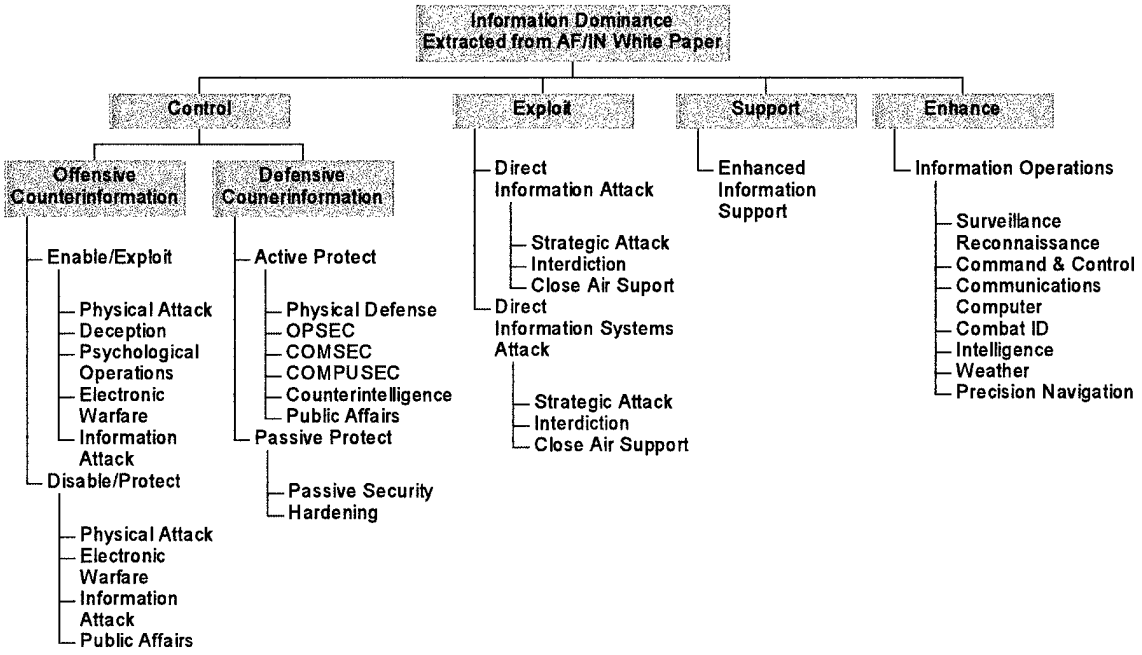

Figure 13: AF/IN White Paper Proposed Information Warfare Doctrine

This hierarchy is similar to existing Air Force doctrine in its objectives. While this provides a level of comfort and, presumably, an assured ability to meet the needs without realignment of functional areas, this hierarchy does not meet the requirements of a value model for IO. Most significantly, *support* and *enhancement* are not mutually exclusive. The definition of information function demonstrates this. "Activities involved in the acquisition, transmission, storage, or transformation of information," will both serve the objectives of enhancement and support—the functions are the same and no clear delimiter is presented to explain how support and enhancement differ. Additionally, it is difficult to understand how one can gain *control* over the information realm in a manner that is mutually exclusive to *exploitation*. The physical systems *exploited* to gain *control* over the information are the same entities that once *controlled* permit *exploitation* by these same means.

The AF/IN White Paper represents great insight into the future of information operations. However, one of the most significant insights is the mapping of the virtual battlespace, defined as an essential task of intelligence. Establishing and maintaining virtual battlespace awareness holistically addresses each intelligence function and each discipline of the existing intelligence process. Then, by maintaining a real-time awareness of the location, status, and intentions of the adversary, a wide asymmetry of awareness is established between friendly and adversary forces—a dominant battlespace awareness. By exploiting this

awareness, the battlespace may be shaped in a manner that constrains the opponent; channeling opposing efforts into a spiraling path of exploitation [Abraham, 1996: 12-13].

Information warfare targeting requirements are addressed as an intelligence function that is now defined as an information function. The need for a quantifiable means of assessing the effectiveness of non-lethal and information warfare specific weapon systems in addition to combat assessment for IW. To produce these measures, AF/IN suggests something similar to JMEMs, which provide kill mechanisms of traditional weapons, vulnerability data, and damage criteria [Abraham, 1996: 19]. While this need is recognized, the means of quantifying these criteria are still unspecified. AF/IN does offer candidate employment concepts as shown in Figure 14. Further, a set of attributes that is proposed as means of measuring merit is offered (see Figure 15).

Candidate IW Employment Concepts

Corruption - The alteration of information content; the manipulation of data to make it either nonsensical or inaccurate. Destroying existing knowledge.

Deception - A specific type of corruption; the alteration of, or adding to, information to portray a situation different from reality. Creating false knowledge to include masquerading.

Delay - The reversible slowing of the flow of information through the system, and the slowing of the acquisition and dissemination of new knowledge.

Denial - The reversible stopping of the flow of information for a period of time, although the information may be transmitted and used within friendly territory, the adversary is denied access to it. The prevention of the acquisition and dissemination of new knowledge.

Disruption - The reduction of the capacity to provide and/or process information (reversible). This is a combination of delay and corruption. The delay of the acquisition and dissemination of new knowledge and the destruction of existing knowledge.

Degradation - The permanent reduction in the capacity to provide and/or process information.

Destruction - The destruction of information before it can be transmitted, the permanent elimination of the capacity to provide and/or process information.

Figure 14: Information Warfare Employment Concepts from AF/IN White Paper

Overall, the AF/IN white Paper served as a guiding light to the future of information operations. With it, a clearer understanding of the revolution in military affairs was presented and because of it, the discussion of systems merit was furthered.

Information Warfare System Attributes

Persistency - How long will the IW strategy affect the target?

Speed - How long will it take to achieve the desired IW effect?

Latency - *Can* the IW tactic lie dormant within the target until needed?

Reversibility - Is the IW effect reversible? Both reversible and irreversible effects can be desirable.

Fratricide - Does the attack method cause unwanted effects on friendly systems?

Collateral Damage - Will attacking the target cause collateral damage in other Systems because of its linkage(s)? Will the method of attack cause unwanted effects on other systems?

Stealth - How easily can an enemy detect the IW attack? Exploitation and corruption of the enemy's information must be accomplished in a manner which is not readily detectable. The effectiveness of the attack is obviously degraded if the enemy gains knowledge of it. (In some cases, it may be beneficial to ensure the enemy knows the friendly information operation capability).

Mutual Interference - Will attacking the target negate other information operations? If the information employment concept is designed to create a false reality, then one must allow the adversary to "see" or "hear" the false reality. Similarly, planners would not want to target a critical node which can be exploited and serves to enhance information available to friendly forces. This attribute. perhaps more thin any other. affirms the need for a fully coordinated and integrated IW strategy concept.

Figure 15: Attributes of Information Warfare Systems from AF/IN White Paper

VI.4. Global Engagement: A Vision for the 21st Century

After Air Force Manual 1-1, Global Reach—Global Power, and Global Presence came Global Engagement: A Vision for the 21st Century. While Global Presence highlighted technology's role in *situational awareness, lethality,* and *strategic agility;* Global Engagement clarifies and enhances the roles that information operations play in Air Force operations [Global Presence, 1995: 12].

Global Engagement established the core competencies of the Air Force as shown in Figure 16. The strategic vision of Global Engagement addresses the entire scope of the Air Force; the people, capabilities, and infrastructure. It is responsive to the requirements of JV 2010; applying Air Force assets and capabilities in direct support of joint operations. Specifically, Full Spectrum Dominance, as defined in JV 2010, depends on the capabilities of modern air and space power; speed, global range, stealth, flexibility, precision, lethality, global/theater situational awareness, and strategic perspective. Information technologies will support Air Force operations under JV 2010. This anticipated level of technological support requires information superiority, however.

Air Force Core Competencies

Air and Space Superiority - Control over what moves through air and space.

Global Attack - The ability of the Air Force to attack rapidly anywhere on the globe at anytime.

Rapid Global Mobility - Providing the nation its global reach; underpinning its role as a global power.

Precision Engagement - The capability that enables our forces to locate the objective or target, provide responsive command and control, generate the desired effect, and retain the flexibility to re-engage with precision when required.

Information Superiority - Enabling air and space power to contribute to the objectives of a Joint force Commander.

Agile Combat Support - Employing Air Force assets to provide global awareness, intelligence, communications, weather, and navigation support to achieve a Joint Team dominant battlefield awareness.

Figure 16: Air Force Core Competencies[15]

To meet the requirement of Full Spectrum Dominance, a truly interactive common battlespace picture is needed [Global Engagement, 1997]. More specifically, dominant battlespace awareness will require integration of joint information assets. Global Engagement predicts an increased importance in IW and IO. Information operations are recognized as both offensive and defensive, with the top IW priority to defend our own information-intensive capabilities. Offensively, operational and tactical IW will continually support information operations in conjunction with other Federal agencies [Global Engagement, 1997].

---

[15] "Global Engagement: A Vision for the 21st Century Air Force," http:/www.af-future.hq.af.mil/21/coret/. downloaded 19 Jan 1997.

Global Engagement presents no hierarchy for direct consumption; however, the hierarchy in Figure 17 is extracted from the values expressed in the text. Looking at the structure of the hierarchy in the context of this study, each objective depends on information dominance to some level. This dependency is less obvious than in other models because one objective is information superiority itself. To avoid double counting, all information operations that support the remaining objectives could be treated, albeit carefully, as mutually exclusive across any single level of doctrine. For example, Information Superiority and Global Attack may be considered mutually exclusive since information operations that are part of Information Superiority enter Global Attack's hierarchy at a lower hierarchical tier. Relying on caveats of this nature to force mutual exclusivity violates the criterion that the decomposed attributes be understandable. Finally, since this doctrine is service specific rather than joint, accepting it as collectively exhaustive is also difficult.

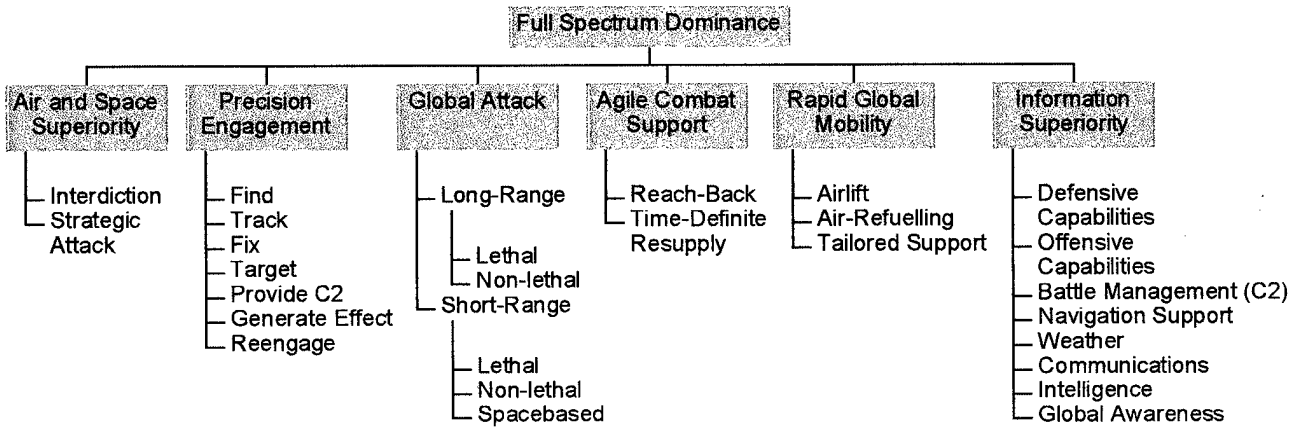

Figure 17: Hierarchy Extracted from Global Engagement

VI.5. Joint Publication 3-13

Building on these predecessors, Joint Publication 3-13, "Joint Doctrine for Information Operations," defines concepts, objectives, and requirements relating to information operations (IO). In Joint Publication 3-13, information is considered a strategic resource that is vital to national security; changing the perspective and treatment of information [Joint Pub 3-13, 1997: I-33]. Additionally, information warfare is split into a continuum of operations; from peace to crisis to war and returning to peace. The difference is that *information operations* are now operations that are conducted continually while IW is conducted only in crisis or war to achieve or promote specific objective over a specific adversary or adversaries [Joint Pub 3-13, 1997: I-1]. The definitions used in Joint Pub 3-13 are presented in Figure 18.

Terminology Used in Joint Publication 3-13

Command and Control - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission.

Command and Control Warfare - The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.

Communications Security (COMSEC) - The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession or study. COMSEC includes cryptosecurity, emission security, and physical security (physical measures).

Computer Network Attack (CNA) - Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Electronic Warfare (EW) - Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. EW includes electronic attack (EA), electronic protection (EP), and electronic warfare support.

Information - Facts, data, or instructions in any medium or form. Also, the meaning that a human assigns to data by means of the known conventions used in their representation.

Information Assurance(IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Environment - The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself.

Information Operations (IO) - Actions taken to affect adversary information and information systems while defending one's own information and information systems.

Information Superiority - The capability to collect, process, and disseminate and uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.

Information System - The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

Information Warfare (IW) - Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

Intelligence Preparation of the Battlespace (IPB) - An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations.

Figure 18: IW Definitions Used in JP 3-13

VI.5.1. Offensive Information Operations

Information operations are both offensive and defensive. Joint Publication 3-13 states that "offensive IO capabilities are employed at every level of warfare, across the range of military operations and will be employed to achieve mission objectives," [Joint Pub 3-13, 1997: II-1]. Information operations are intended to affect the adversary's information or information systems and can yield a tremendous advantage to US military forces during times of crisis and conflict.

Offensive IO applies traditional perception management disciplines to produce a synergistic effect against the elements of an adversary's information systems. OPSEC, PSYOP, deception, electronic warfare, physical destruction (elements of C2W), public affairs (PA), and civil affairs (CA) can all be integrated and/or applied synergistically to ensure success [Joint Pub 3-13, 1997: II-14]. The level of effort and disciplines employed are as much a function of the level of IO intensity as the synergistic effects of the disciplines already employed (see Figure 19).

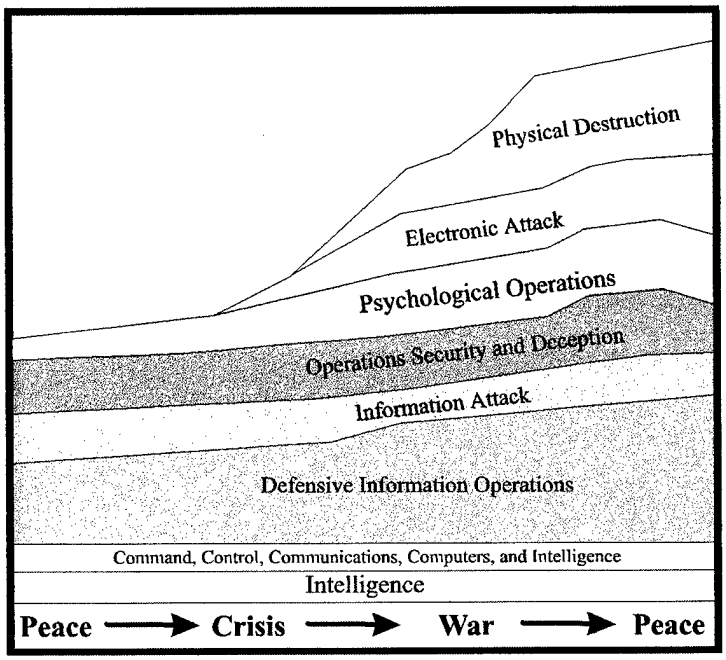

Figure 19: Information Operations Engagement Timeline[16,17]

Joint Publication 3-13 outlines the potential impact of offensive IO in peace and in military operations other than war (MOOTW). These situations present opportunities to yield the greatest impact from perception management and the influencing of an adversary's decisionmaking. The rationale for this stems from the initial goal of IO; maintaining peace, defusing crisis, and deterring conflict. As tensions increase, and the situation or circumstances move toward conflict, the ability to target and engage critical adversary information and information systems decreases. This is compounded by the increased criticality of and value placed on the information and information systems by an adversary[Joint Pub 3-13, 1997: II-14].

[16] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-15.
[17] The line separating Electronic Attack and Psychological Operations is this author's guess. The original line was illegible in the draft form of the publication.

This movement within the pre-crisis level of military operations also causes some changes in objectives for offensive IO (refer to Table 4). As with the range of military operations, the level of operation also affects the objectives (see Table 5). The objectives are also shown in Figure 20 on a sliding scale of the conflict continuum versus the predicted objectives.

Table 4: Range of Military Operations Vs Objective[18]

Range	Potential Objective
Peace	• Deter crisis • Control crisis escalation • Project power • Promote peace • Battlespace preparation
MOOTW	• Maintain peace • Defuse crisis • Deter conflict • Preparation of battlespace
Conflict and War	• Degradation or destruction of adversary information systems and their (human element) will to fight • Help dominate combat operations and influence the adversary to terminate hostilities on terms favorable to the US

Table 5: Level of Operations Vs Objective[19]

Level	Objective
Strategic	• Engage adversary or potential adversary leadership to deter crisis and end hostilities once they occur. (actions against elements of adversary national power; political, military, economic, and informational)
Operational	Focused on adversary or potential adversary in combatant commander's area of responsibility (AOR) • Maintaining peace • Deterring crisis • Failing deterrence, supporting quick resolution of hostilities on terms favorable to the United States
Tactical	Conducted by Joint Task Force commander with in assigned joint operations area • Deny or disrupt adversary's use of information and information systems relating to C2, intelligence, and other critical information-based processing directly related to conducting military operations • Affect the will of an adversary's forces to resist • Deny an adversary's use of the affected populace for advantageous purposes

Beyond the crisis point of relations, IO can serve as a force enabler, affecting every aspect of an adversary's decision cycle by impacting its information centers of gravity [Joint Pub 3-13, 1997: II-17]. While defining the span of information operations, Joint Publication 3-13 also limits the use of indiscriminate employment of information operations by stating that ; "[the] selection and employment of specific offensive IO capabilities against an adversary should be appropriate to the situation with the adversary(ies) and US objectives and consistent with applicable international conventions and standing rules of engagement," [Joint Pub 3-13, 1997: II-2]. Avoiding indiscriminate operations requires precise capabilities. To this end, IO precision is implicit in the sixth principle of offensive IO (Figure 21); requiring that discrete portions of an adversary's information or information systems be identified and targeted and the prediction of the consequences of employing specific offensive capabilities prior to an information or information systems attack [Joint Pub 3-13, 1997: II-2-II-3]. These

[18] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-14-II-17.

targeting objectives are shown in Table 6.

Joint Publication 3-13 states that offensive IO can be effective against all elements of national power and that all elements should be considered with respect to desired objectives when targeting [Joint Pub 3-13, 1997: II-25]. To this end, three target areas are identified, the human decision process, the information and information systems used to support decisionmaking, and the information and information systems to implement the decisions made [Joint Pub 3-13, 1997: II-25].

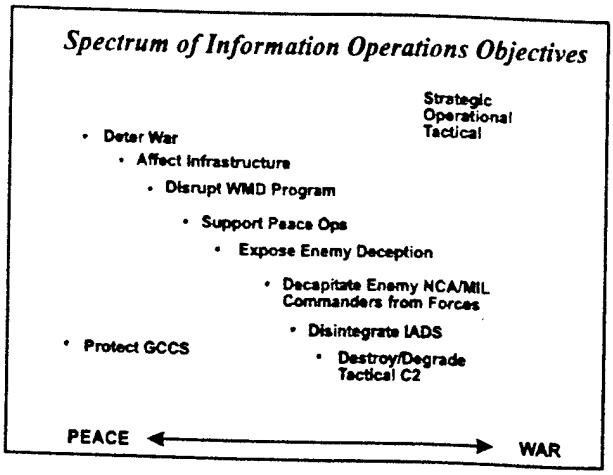

Figure 20: IO Objectives[20]

Principles of Offensive Information Operations

1 The human and associated decisionmaking processes are the ultimate target for IO. Offensive IO are employed as an integrating strategy that orchestrates varied disciplines and capabilities into a coherent, seamless plan to achieve specific objectives.

2 Offensive IO objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.

3 Selection and employment of specific offensive capabilities against an adversary should be appropriate to the situation with the adversary(ies) and US objectives and consistent with applicable international conventions and standing rules of engagement.

4 Offensive IO may be the main or supporting element of a JFC's campaign or operation.

5 Offensive IO in support of a JFC's campaign or operation may include planning and execution by non-DOD forces, agencies, or organizations and must be thoroughly synchronized, coordinated, and deconflicted with other aspects and elements of the supported campaign or operation.

6 In order to adequately attack information and information systems, it is necessary to be able to do the following:

a. Determine the adversary's valuation, use, and flow of information.
b. Identify and target discrete portions of an adversary's information or information systems.
c. Predict the consequences of employing specific offensive capabilities with a predetermined level of confidence.
d. Evaluate the outcome of specific IO attacks with confidence.

Figure 21: Principles of Offensive Information Operations[21]

[19] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-18-II-21.
[20] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-3.
[21] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-1-II-3.

Joint Publication 3-13 recognizes the potential eventuality that offensive IO against adversary information systems and their will (human element) to fight may not take place in the same physical battlespace or be conducted in the same time frame as the combat operations they support. Despite this, these operations must be thoroughly synchronized with the supported combat operations [Joint Pub 3-13, 1997: II-19]. Part of this synchronization involves strategic targeting operations.

Table 6: Targeting Objectives[22]

Targeting Level	Target Objectives
Strategic	To act on an adversary's center(s) of gravity within the elements of national power: • Deter Adversary or potential adversary from actions leading to the outbreak of hostilities or other activities (military or non-military) not in the best of the US
Response	Support in initial IO objectives and follow-on attacks based on BDA or support of defensive IO

Strategic targeting of IO may involve direct, indirect, and supporting attacks. The authors of Joint Publication 3-13 state that most targeting will involve direct attacks on the information and information systems within the elements of national power that will cause an adversary or potential adversary to make decisions favorable to the US. Further, most offensive IO targeting is expected to be a logical extension of the peacetime IO planning [Joint Pub 3-13, 1997: II-26-II-27].

[22] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. II-25-II-28.

VI.5.2. Defensive Information Operations

Defensive information operations coordinate protection and defense of the information, information-based processes, and information systems critical to military operations [Joint Pub 3-13, 1997: III-1]. Using this description, the human decisionmaking processes are included as an information-based process and the information systems include traditional C4 systems, weapon systems and infrastructure systems. Protection is offered by integrating and coordinating policies, procedures, operations, personnel, and information assurance technology. Timely, accurate, and relevant information access are ensured while denying access by an adversary to friendly systems [Joint Pub 3-13, 1997: III-2].

Information assurance (IA) is a new term. IA protects and defends information and information systems by ensuring their availability, integrity, identification, and authentication, confidentiality, and non-repudiation to include information system restoration. The means of information assurance include protection, detection, and reaction capabilities employing firewalls, secure servers, and intrusion detection software [Joint Pub 3-13, 1997: III-2-III-3].

To implement IO under Joint Pub 3-13, defensive IO must operate in conjunction with offensive IO, this is represented in the hierarchy extracted from Joint Publication 3-13, shown in Figure 22. Integration will

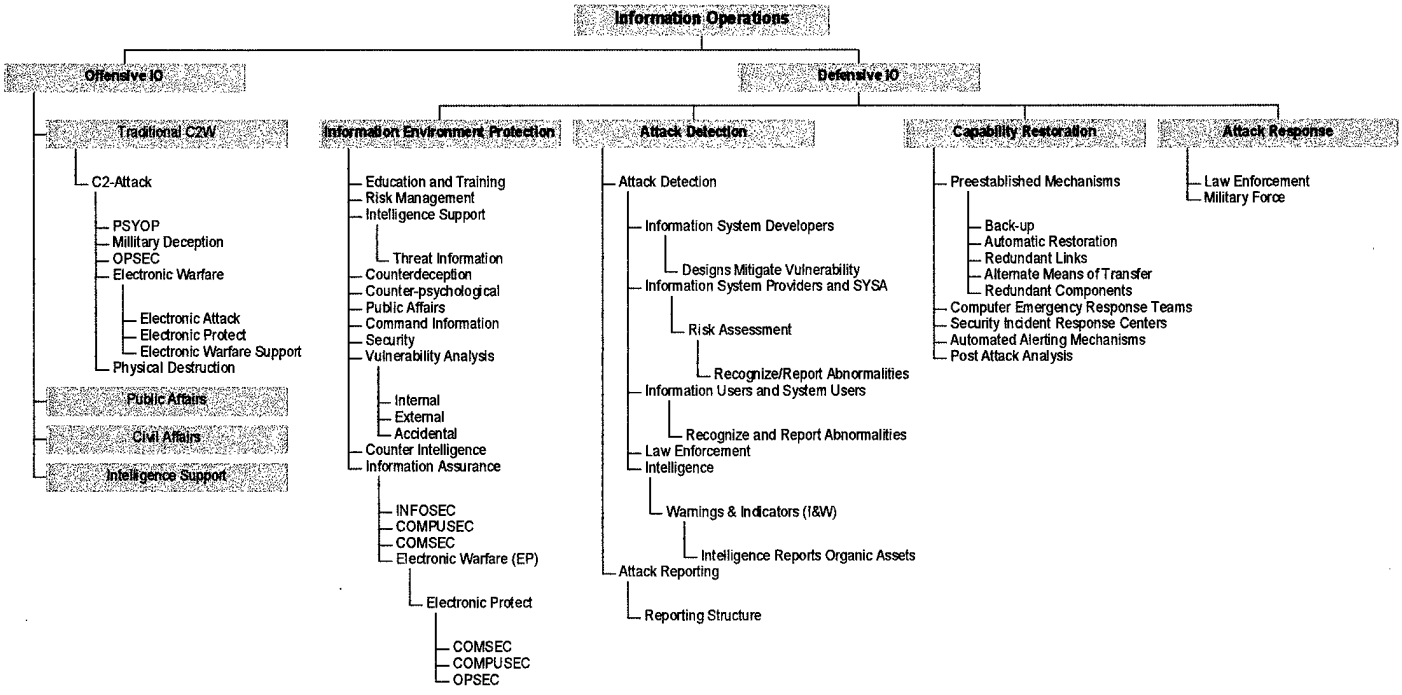

Figure 22: Information Operations Hierarchy extracted from Joint Publication 3-13

provide timely response to potential threats. Complete integration (presumably from training through practice and employment cycles) as outlined in Joint Pub 3-13 anticipates that the four central processes of defensive IO—*protect, detect, restore,* and *respond* are uniformly.

The scope of these defensive measures is larger than the uniformed services themselves; requiring close cooperation between military and non-military organizations (also shown in Figure 22). The scope is more formally addressed as the *information environment*—bounded by what is critical to joint force operations [Joint Pub 3-13, 1997: III-6].

The *information environment* that is critical to the joint force is a combination of physical systems and facilities, and the more abstract intelligence processes. The protection of this environment is rooted in risk management; assessment of information needs, value, and system vulnerabilities; all of which can change from one military phase to the next [Joint Pub 3-13, 1997: III-6-III-7]. Joint force commanders implement an *information environment protection* process by developing common policies, procedures, establishing technical capabilities, and focusing operations, to include defensive IO objectives [Joint Pub 3-13, 1997: III-8].

The procedures to implement defensive IO include education, training, and awareness; risk management; intelligence support (threat assessment), counterdeception operations, counter-psychological operations, Public Affairs, command information programs, security, vulnerability analysis and assessments, and by applying Information Assurance (IA) capabilities (information security, computer security, communication security, and electronic protection) (Figure 22) [Joint Pub 3-13, 1997: III-6-III-16].

The detection process is addressed by the *Attack Detection Process* in Joint Publication 3-13. The speed and range of information attacks has generated the need for automated detection and automated threat-mitigation systems. Timely attack detection and reporting are the keys by which to initiate restoration and the attack response processes [Joint Pub 3-13, 1997: III-16]. The identified elements of the attack detection process include; information system developers, information system providers and administrators, information users, information system users, law enforcement, and intelligence [Joint Pub 3-13, 1997: III-16-III-17]. The role of intelligence includes intelligence support functions including indicators and warnings, threat assessment process, probability of adversary IO actions, and adversary capabilities, intents, motives, goals, objectives, dispositions, military and non-military IO activities, and mobilization

status [Joint Pub 3-13, 1997: III-17-III-20].

For attack indicator and warnings and threat assessments to be effective, they must be disseminated. The need is, then, for a reporting structure designed to alert managers and administrators at all levels of abnormalities. The systems structure to be linked to intelligence, law enforcement, policy makers, and the information systems community, both government and commercial [Joint Pub 3-13, 1997: III-20].

The restoration process of defensive IO is termed the *Capability Restoration Process*. This relies on preestablished mechanisms to form prioritized restoration of minimum essential capabilities [Joint Pub 3-13, 1997: III-20]. The means include, information backup, redundant links, or even alternative means of information transfer [Joint Pub 3-13, 1997: III-21]. Emergency response teams have formed termed by Joint Pub 3-13 as Computer Emergency Response Teams (CERTs) to repair and mitigate attack damages. Further, on-line or deployable restoration assistance is entering into restoration processes. Situational awareness is provided, in part, by automated alerting mechanisms that protect and alert. System resources inventory is also identified as a means to detect implanted weapons. Finally, post-attack analysis will provide vulnerability assessment; aiding in future protection [Joint Pub 3-13, 1997: III-21-III-23].

The final process of defensive IO is the *Attack Response Process*. The *Attack Detection Process* triggers the response process. Once triggered, the actors and motives are assessed, establishing cause and complicity. Attack response directly counters information attack threats and enhances deterrence [Joint Pub 3-13, 1997: III-23]. The level of deterrence is subject to national-strategic decisions regarding the application of flexible deterrent options. The response options include law enforcement and military forces [Joint Pub 3-13, 1997: III-24].

The structure of the hierarchy extracted from Joint Publication 3-13 is substantially different from that of Joint Publication 3-13.1. The extracted hierarchy appears to meet the requirements of an objectives hierarchy, subject to delineation of the means objectives. Potential conflict exists between the *Information Environment Protection* and *Attack Detection* and *Attack Response*. Counterpsychological and counterdeception operations may not be mutually exclusive with *Attack Response*. Intelligence support to *Information Environment Protection* may not be mutually exclusive to Intelligence in *Attack Detection*. These and other questions are answered by framing the decision and associating means objectives with the fundamental objectives as proposed in Figure 22.

A similar question occurs on the offensive IO side of the figure—is OPSEC mutually exclusive with the rest of the objectives or is it a means for all others? This question is addressed by reviewing the Joint Publication on C2W, since this part of the hierarchy stems from that document. In fact, Joint Publication 3-13 explicitly references Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W) as part of the current structure. Because of this, the final step in forming the initial decision frame is to review C2W doctrine.

VI.6. Joint Publication 3-13.1

With the definitions either being developed or replaced by new definitions in Joint Publication 3-13, the level of development and analysis of C2W doctrine will be more terse; focusing on the values represented in the document. The scope of this document is represented by the definition of C2W; the integrated use of psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions [Joint Pub 3-13.1, 1996: v.].[23]

Joint Pub 3-13.1 identifies the overall strategic target of C2W as the information dependent process, whether human or automated [Joint Pub 3-13.1, 1996: I-5]. This is extended by the identification of people, decisionmakers at all levels, as the most important part of any information system [Joint Pub 3-13.1, 1996: I-1]. The definition of information systems is similar to that found in Joint Publication 3-13; similar enough to be interchangeable for the purposes of this paper.

As for the scope of operations, three categories of the information infrastructure are defined in Joint Publication 3-13.1; the global information infrastructure (GII), the national information infrastructure (NII), and the defense information infrastructure (DII). The GII is the worldwide interconnection of communications networks, computers, databases, and consumer electronics that make information available to users [Joint pub 3-13.1, 1996: I-2]. This definition includes the people who operate and consume the information as a critical component of the GII. While no specific delineation of the NII is presented, the definition of DII is clarified. The DII is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving the DOD's local, national and worldwide information needs [Joint Pub 3-13.1, 1996: I-3]. These definitions serve as a means to discern the ownership of systems and processes, though all three are inextricably intertwined, making all relevant to IO.

C2W is defined to be an application of information warfare, now termed information operations. As such, it is composed of both offensive and defensive actions; C2-attack and C2-protect. The range of C2W

[23] Joint doctrines exist for many of the elements of C2W: unclassified ones will be used to support increasing levels of detail in the latter developments of this paper but will be excluded in the framing of the decision model.

operations is best represented in Figure 23. The extracted hierarchies for both offensive and defensive C2W as part of the larger C2W hierarchy are shown in Figures 24 and 25.

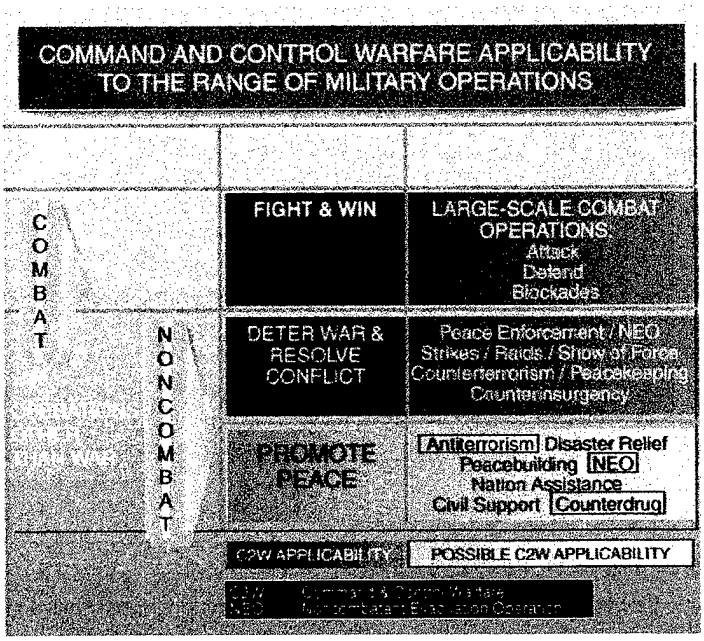

Figure 23: Command and Control Warfare Applicability to the Range of Military Operations[24]

Within theater operations, effective C2W provides the joint force commander the ability to shape the adversary commander's estimate of the situation. Further, successful C2W will contribute to the security of friendly forces, bring the adversary to battle (if appropriate) at a disadvantage, help seize and maintain the initiative, enhance freedom of maneuver, contribute to surprise, isolate the adversary forces from their leadership, and create opportunities for a systematic exploitation of adversary vulnerabilities [Joint Pub 3-13.1, 1996: I-5-I-6]. Effective C2W operations will also influence, disrupt, or delay the adversary's decision cycle. By synchronizing C2W operations it should be possible for the joint force commander to operate inside the adversary's decision cycle [Joint Pub 3-13.1, 1996: I-6]. To enable exploitation of these opportunities, OPSEC, PSYOP, military deception, electronic warfare, and physical destruction must be understood and integrated. To this end, the definitions and objectives are summarized in Figure 26. Treating these definitions and objectives a an exhaustive set, the formal decision opportunity framing is completed, leading to the formation of the value hierarchy.

[24] Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 1996, p. I-5.

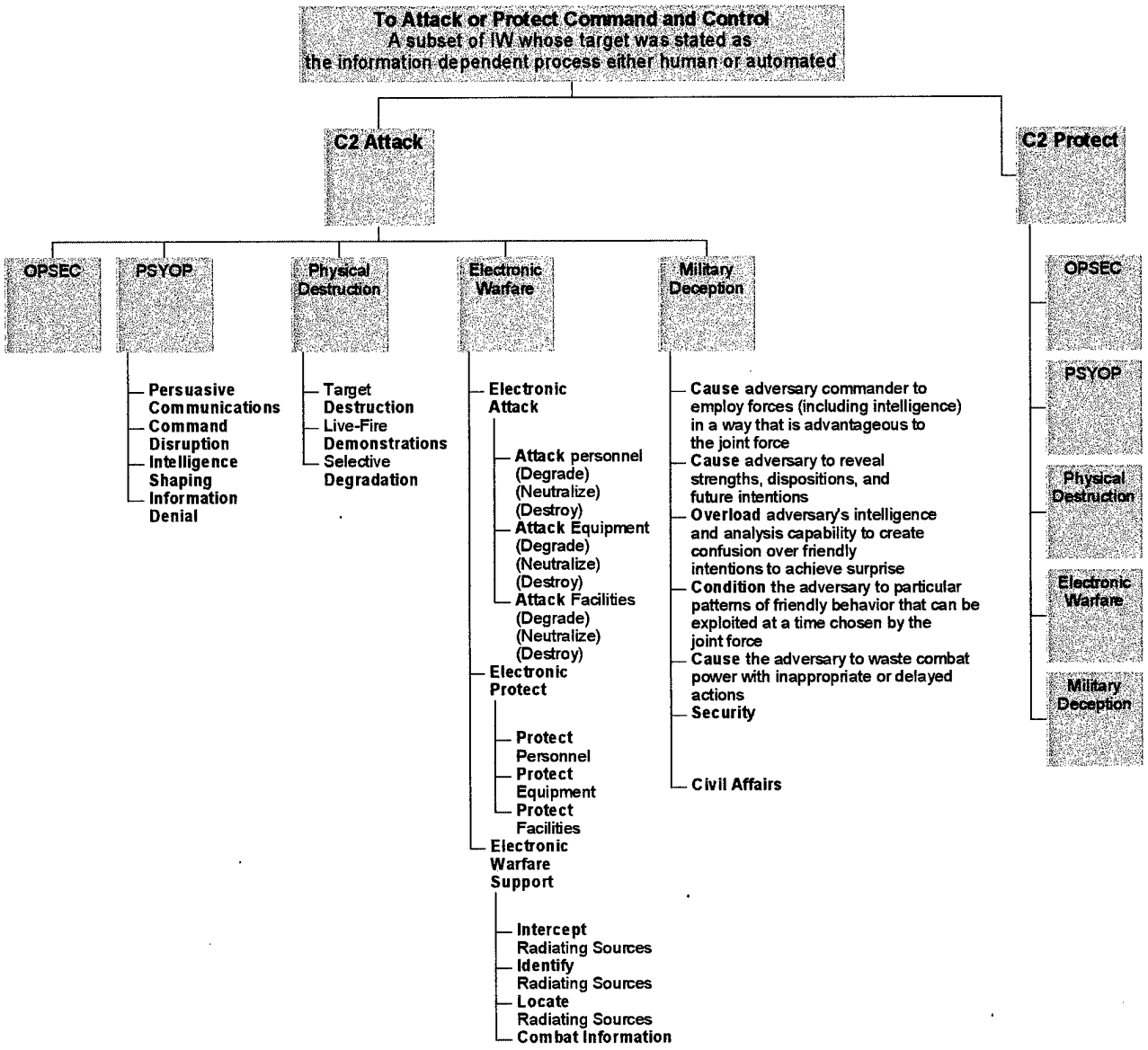

Figure 24: C2W Extracted Hierarchy: C2 Attack

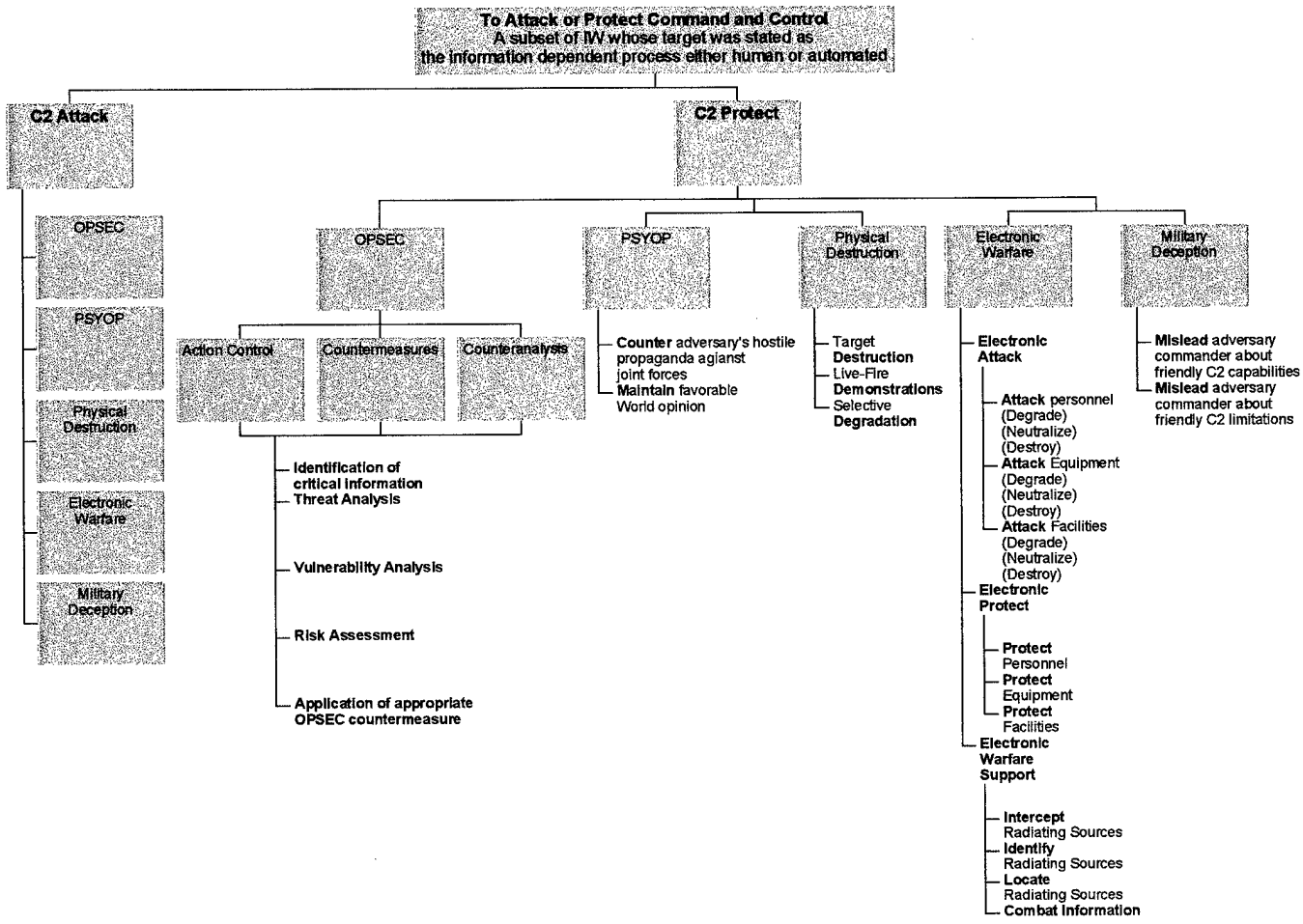

Figure 25: C2W extracted Hierarchy: C2 Protect

Elements of Command and Control Warfare

OPSEC - OPSEC is concerned with denying critical information about friendly forces to the adversary. In C2W, this threat is ultimately the adversary commander. The intent of OPSEC in C2W should be to force the adversary commander to make faulty decisions, based on insufficient information and/or to delay the decisionmaking process due to a lack of information. Additionally, OPSEC planners must work closely with public affairs (PA) to avoid disclosure of critical information. Critical information can be hidden by traditional measures such as action control, countermeasures, and counteranalysis.

PSYOP - PSYOP can influence attitudes, emotions, motives, objective reasoning, and ultimately, the behavior of foreign governments, their leaders, groups, and individuals. PSYOP in support of C2-attack can articulate to appropriate foreign audiences the mission, intent, and combat power of the joint force, as well as curb unreasonable expectations about the US government's role and actions during operations. It can also multiply and magnify the effects of military deception, reinforce apparent perceptions of the adversary, sow doubt about adversary leadership, proliferate discrete messages to adversary command, control communications and intelligence collectors, enhance and combine live fire demonstrations with surrender appeals, and magnify the image of US superiority. PSYOP's main objective in support of C2-protect is to counter the adversary's' hostile propaganda against the joint force and to maintain a favorable world opinion of the operations. As a corollary, PSYOP can drive a wedge between the adversary leadership and its populace. Information packets can also be developed by PSYOP specialists to immunize friendly units against adversary propaganda.

Military Deception - As an element of C2, military deception should focus on causing the adversary commander to estimate the situation with respect to friendly force disposition, capability, vulnerability, and intent incorrectly. Some goals of military deception in support of C2-attack include: causing the adversary commander to employ forces (including intelligence) in ways which are advantageous to the joint force; Causing the adversary to reveal strengths, dispositions, and future intentions; overload the adversary's intelligence and analytical capability to create confusion regarding friendly intentions and to achieve surprise; to condition the adversary to particular patterns of friendly behavior that can be exploited at a time chosen by the joint force; and to cause the adversary to waste combat power with inappropriate or delayed actions. In support of C2-protect, can help protect the joint force from C2-attack by misleading an adversary commander about friendly C2 capabilities and/or limitations.

Electronic Warfare - Electronic warfare is composed of three elements, electronic attack (EA), denying an adversary use of the electronic spectrum; electronic protection (EP), guaranteeing the use of the electromagnetic spectrum to the joint force commander; and electronic warfare support (ES), contributing to the joint force commander's accurate estimate of the situation in the operational area. In support of C2-attack, ES in the form of combat information can provide real-time information required to locate and identify C2 nodes and supporting systems. ES can also support SIGINT production. EA in support of C2-attack can be in the form of jamming, electromagnetic deception, and C2 node destruction. EP in support of C2-attack protects the electromagnetic spectrum for friendly use through employment of the Joint Restricted Frequency List. Electronic warfare in support of C2-protect also employs all three elements. ES in support of C2-protect can be used to monitor for impending adversary attack on C2 nodes. EA in support of C2-protect can be in the forma of jamming, electromagnetic deception, or directed energy weapons or antiradiation missiles. EP in support of C2-protect safeguards friendly forces from exploitation via SIGINT and prevents conflicts by employing the Joint Restricted Frequency List.

Physical Destruction - Physical Destruction, as an element of C2W refers to the use of "hard kill" weapons against designated targets as an element of an integrated C2W effort. Although the word "destruction" is used in the term, "hard kill" weapons may be used in C2W for a purpose other than the actual destruction of a specific target. Firepower demonstrations or selective degradation of certain parts of a C2-related target through weapons effects are examples of the use of "hard kill" weapons for a purpose other than actual destruction that might be part of an integrated C2W plan. Normally, physical destruction would target identified C2 nodes. However, physical destruction may also be against targets other than adversary C2 nodes in support of one or more of the other elements of C2W.

Figure 26: The Elements of C2W[25]

[25] Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 1996, pp. II-1-II-8.

VII. Framing the Decision

As defined earlier, a decision is framed by defining both the decision context and the strategic objective this was represented in Figure 27. With all the necessary textual review completed, we now proceed to frame the decision and develop a value hierarchy for the information realm.

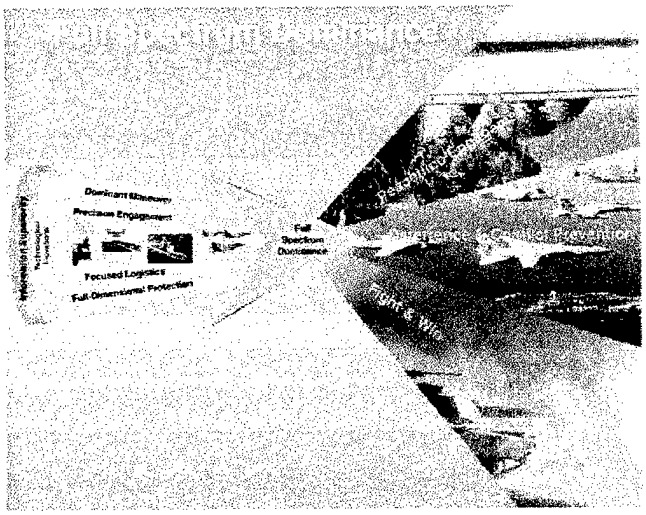

Figure 27: Full Spectrum Dominance, The Strategic Objective of Joint Vision 2010[26]

VII.1. Selecting a Decision Context

In selecting the decision context it is reasonable to select the largest possible context, in fact it is the reason for selecting value-focused thinking in the first place. The broadest of all the implied and stated contexts is that of Joint Publication 3-13. Information is to be considered a strategic resource, vital to national security [Joint Pub 3-13, 1997: I-33]. Information warfare is divided into information operations and information warfare associated with a continuum of conflict. Information operations are conducted continually both defensive and offensive [Joint Pub 3-13, 1997: II-1]. This requires an expansion of decision context, beyond what was argued earlier as the span of control of the military (see Figure 28). In the text of Joint Publication 3-13, the support of national military strategy is stated to require the support, coordination, and participation by other US government agencies as well as commercial industry. Further, it is stated that while DOD information flows depend on commercial infrastructures, the protection of these falls outside the authority and responsibility of the DOD [Joint Pub 3-13, 1997: I-22]. This must be included in the information environment, the global, national, and defense information infrastructures (GII, NII, and DII respectively).

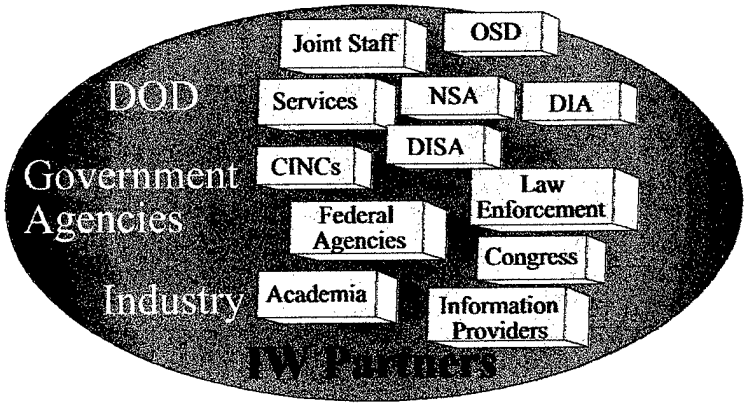

Figure 28: Partners in IW[27]

[26] Joint Vision 2010, OPR, chairman of the Joint Chiefs of Staff, Pentagon, Washington, DC 20318-5126, p. 26.

The other parts of this context are those things that are valued. Defensively, the information, information systems, and information-based processes within the GII, NII, and DII are those elements important to national security. Offensively, the adversary decisionmakers or potential adversary decisionmakers are important. In both cases, accessibility is via information, information systems, and information-based processes. While defining these terms limits the scope, the scope must still be broad enough to cover the entire information environment, as defined in Figure 29.

Definitions Used to Help Define the Decision Context

Information - Facts, data, or instructions in any medium or form. Also, the meaning that a human assigns to data by means of the known conventions used in their representation (Joint Publication 1-13 and 3-13.1). Data and the instructions required to give that data meaning (AF/IN White Paper)

Information System - The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual (Joint Publication 3-13.1). The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information (Joint Publication 3-13 and 3-13.1). Joint Publication 3-13, however, defines the information system to include the information-based processes or sub-processes (Joint Publication 3-13). Any physical component used to acquire, transmit, store, or transform information (AF/IN White Paper).

Information-Based Processes - Processes that collect, analyze, and disseminate information using any medium or form. These processes may be stand-alone processes which, taken together, comprise a larger system or systems of processes. Information-based processes are included in all systems and components thereof that require facts, data, or instructions in any medium or form to perform designated functions or provide anticipated services (Joint Publication 3-13). The activities involved in the acquisition, transmission, storage, or transformation of information (AF/IN White Paper).

Information Environment - The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself (Joint Publication 3-13)..

Figure 29: Collective Definition Used to Frame the Decision[28,29,30]

It is proposed that the information environment is spanned by information, information-based processes, and information systems. This author believes that information-based processes and information systems are distinctly different. These are differentiated by requiring that information-based processes add value to information with respect to the decisionmaking processes and that information systems act on and return information without adding value to the decisionmaking processes. Presenting an alternate and equivalent definition of information from those previously offered, information is defined for this analysis as data and the semantic meaning, presenting an opportunity to more readily identify information from the information functions that support information-based processes.

[27] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. I-23.
[28] Joint Publication 3-13 (Draft), Joint Doctrine for Information Operations, 21 Jan 1997, p. I-17, I-19.
[29] Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 1996, p. GL-8.
[30] Abraham, Arnold, "Air Force Intelligence and Information Warfare," AF/IN White Paper, 1 Mar 1996, p. 6.

Finally, by applying these definitions, a decision context is offered: The information, information systems, and information-based processes that are important to national security, permit the ability to access and influence adversary or potential adversary and friendly decisionmakers either human or automated. Accepting along with this decision context, a caveat, that is identified in Joint Publication 3-13; "IO may involve complex legal and policy issues requiring careful review and national-level coordination and approval," [Joint Pub 3-13, 1997: I-2].

VII.2. Selecting a Strategic Objective

From a joint perspective, Joint Vision's Full Spectrum Dominance is the overarching strategic objective, accomplished through successful implementation of the four operational concepts identified in JV 2010 (Figure 27) [JV 2010, 26]. Full Spectrum Dominance implies that all realms (air, land, sea, space, and information) will be dominated. Using this, then the fundamental objective of IW that serves as its component of the joint hierarchy is "to dominate the information realm." Using the definition of Joint Publication 3-13, that information is a critical resource, and the declarations in both the AF/IN White Paper and Cornerstones of Information Warfare that information is indeed a separate realm, this seems acceptable as on overarching strategic objective [Joint Pub 3-13, 1997: I-33] [Abraham, 1996: 11] [Widnall: 2].

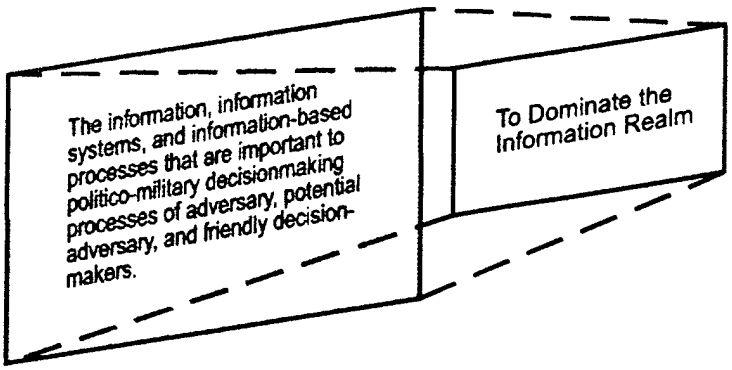

Figure 30: Proposed Decision Frame

The proposed decision frame is shown in Figure 30 by projecting the strategic objective (to dominate the information realm) onto the set of all acceptable and feasible alternatives for accomplishing the strategic objective. These alternatives are conceptually the information, information systems, and information-based processes that are significant to the military decisionmaking processes, both friendly and hostile.

VIII. Forming the Value Model

While all the documents reviewed present objectives for information warfare either directly or implicitly, none provide a fundamental value hierarchy that is directly applicable to a VFT analysis. Joint Publication 3-13 is closest to meeting this requirement and will serve as the basis for much of the work to follow.

Recalling that a value hierarchy requires objectives that are mutually exclusive and that collectively fulfill the strategic objective in an exhaustive manner, a value hierarchy if formed from the values extracted from the reviewed "gold standards." To this end, the doctrinal documents mentioned previously have been fit into a hierarchical network with respect to the originating authority, chronological release, an scope. This network demonstrated that none of the doctrines met the requirements of a pure value hierarchy. They also demonstrated that information is as different of a realm as air, space, land, and sea. Analysis demonstrated that at the highest level of joint doctrine, information superiority is not independent of dominant Maneuver, Precision Engagement, Full-Spectrum Protection, and Focused Logistics; indicating that information warfare value model must be sought outside of this context. With no doctrine existing that meets these criteria directly, a value hierarchy must is created as a preliminary step in the process of developing measures of merit using VFT.

VIII.1. The Information Realm

The Air Force Intelligence White Paper titled "Information Warfare" divides the information realm into three elements; information (data and semantic meaning), information systems (systems that convey, store, collect, disseminate information with out adding value), and information functions (actions/enhancements that add value to the information). These three elements initially appear to be collectively exhaustive and mutually exclusive and consistent with other doctrinal publications.

VIII.2. Battlespace Awareness

It is also useful to align these three elements with other common definitions that are both currently accepted and reflect, in part, the values of the decisionmakers. To this end, the proposed decision frame element of *information-based processes;* defined as a processes that add value to information (data and semantic meaning), is considered with the concepts of *dominant battle-space awareness* from JV 2010 and *intelligence preparation of the battlespace (IPB)* from Joint Publication 3-13. For consistency, the concepts of mapping the virtual battlespace are included from the AF/IN White Paper and the commander's estimate is included from Joint Publication 3-13.1. The definitions and appropriate discussions from the

Definitions Related to Information-Based Processes

Dominant Battlespace Awareness - Improvements in information and systems integration technologies will also significantly impact future military operations by providing decisionmakers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistics support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations. Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it [JV 2010:13].

Intelligence Preparation of the Battlespace - An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate. The database is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process [Joint Pub 3-13: GL-12].

Mapping the Battlespace - Real-time awareness of the location, status, and intentions of the adversary, established by penetrating his virtual landscape to include communication networks, nodes, computer technology, and cognitive interaction [Abraham: 11].

Commander's Estimate of the Situation - A logical process of reasoning by which a commander considers all the circumstances affecting the military situation and arrives at a decision as to a course of action to be taken to accomplish the mission. A commander's estimate which considers a military situation so far in the future as to require major assumptions is called a commander's long-range estimate [Joint Pub 3-13.1: GL-5].

Figure 31: Existing Definitions Associated with Information-Based Processes

parent documents are presented in Figure 31.

Dominant battlespace awareness (DBA), though not formally defined in JV 2010, is described as an interactive picture which will yield much more accurate assessments of friendly and enemy operations within the area of interest. The exact quote, in context, is presented in Figure 31. If this could be an overarching objective, then the other desired consequences; intelligence preparation of the battlespace and mapping the virtual battlespace could be expected to all support DBA. Examining the definitions of each, DBA seems inclusive of IPB, mapping the virtual battlespace, and affecting the commanders estimate; and IPB, mapping the virtual battlespace, and affecting the commander's estimate are supportive of DBA. No attempt is made to demonstrate either mutual exclusivity or that these are collectively exhaustive; decisionmakers are required for that.

Doctrine supports the concept of dominant battlespace awareness both at the conceptual level and operational level. Operational-level objectives that support the proposed overarching objective of dominant battlespace awareness can, therefore, also be found in existing doctrine. The strongest single candidate doctrine to support this is Joint Publication 3-13 represented in Figure 22.

The three proposed elements of the information realm also suggest that the remaining components of the decision context, the information itself and the information systems that collect, store transmit and disseminate the information are items that must be controlled to dominate the information realm—controlling the critical resource of information.

VIII.2.1.Information Systems

The information systems of interest are those that are important to national security, as shown in the decision context, Figure 30. Information systems are defined as shown in Figure 32. These definitions are coherent and mutually supportive. As noted in Figure 29, however, there is a split in definition regarding the inclusion of information-based processes in Joint Publication 3-13. This paper will treat these two elements as separate

Definitions of Information Systems

Information System - The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information [Joint Pub 3-13: GL-11].

Information System - The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. In information warfare this includes the entire infrastructure, organization, and components that collect, process, transmit, display, disseminate, and act on information [Joint Pub 3-13.1: GL-8].

Figure 32: Information Systems Definitions

entities as discussed earlier.

The means for addressing information systems extends from C2W doctrine and is further evolved in information operations doctrine. These means are well considered within these documents; therefore, these documents should be considered as a defining set of minimum requirements to be met in order to maintain military sufficiency. The hierarchies for these are represented in Figures 22, 24, and 25.

VIII.2.2.Information as a Strategic Resource

In relational database theory, the minimum unit of measure is the *scalar:* defined as the smallest unit of semantic data [Date, 1995: 55]. This means that the smallest "atomic" bit of information that is useable must contain a value and have an associated meaning to that value; much like a vector. Separating the meaning from the value leaves no useful information.[31] Other definitions previously examined are shown in Figure 33. These are all consistent with the definition offered above.

Information Definitions
Information - Facts, data, or instructions in any medium or form [Joint Pub 3-13.1: GL-8].
Information - 1. Facts, data, or instructions in any form. 2. The meaning that a human assigns to data by means of the known conventions used in their presentation [Joint Pub 3-13: GL-10].
Information - Data and the instructions required to give that data meaning [Abraham: 8].

Figure 33: Information Definitions

This, then, provides a means of testing and classifying information, functions, and systems based on a set of mutually exclusive definitions. Using the definition of information as data plus the semantic information required to give meaning to the data, anything that affects either the data or the semantic meaning is affecting information. Anything that conveys, stores, or manipulates (transforms data or signals for processing) information in a manner that does not add value to the information in the context of the decisionmaking processes is an information system. Finally, anything that adds value to the decisionmaking process is an information-based process. These developed criteria are both defined and represented by objectives in Table 7. Employing this set of definitions then assures mutual exclusivity and since the definitional elements of the information realm (the information, information systems, and information-based processes) span the information realm, this set is also collectively exhaustive. A hierarchy for this proposed model is shown in Figure 34. In this model, Information-based processes are

[31] An example of this is to consider the following: an envelope is received with the only "8" on the front. This tells the recipient too little information to interpret the meaning. If, however, the user knows it is in context to Numbered Air Forces the recipient can understand this to mean it goes to the 8th Air Force. If either the context or value are missing, or altered, an incorrect action will likely follow in response.

represented as dominant battlespace awareness. This is justified by applying the definition of DBA from Figure 31, and the previous discussion of DBA. This definition relies on data (information) fusion to provide assessments of friendly and enemy operations. Supporting DBA are the elements termed mapping of the battlespace and intelligence preparation of the battlespace. All of these require data fusion to support the decisionmaking processes. By definition, then, these are all information-based processes that impact military decisionmaking. All elements of our current information-based processes, from intelligence to alert rate reporting and maintenance logs, improve our DBA, making DBA collectively exhaustive of all information-based processes that are employed in the military decisionmaking processes.

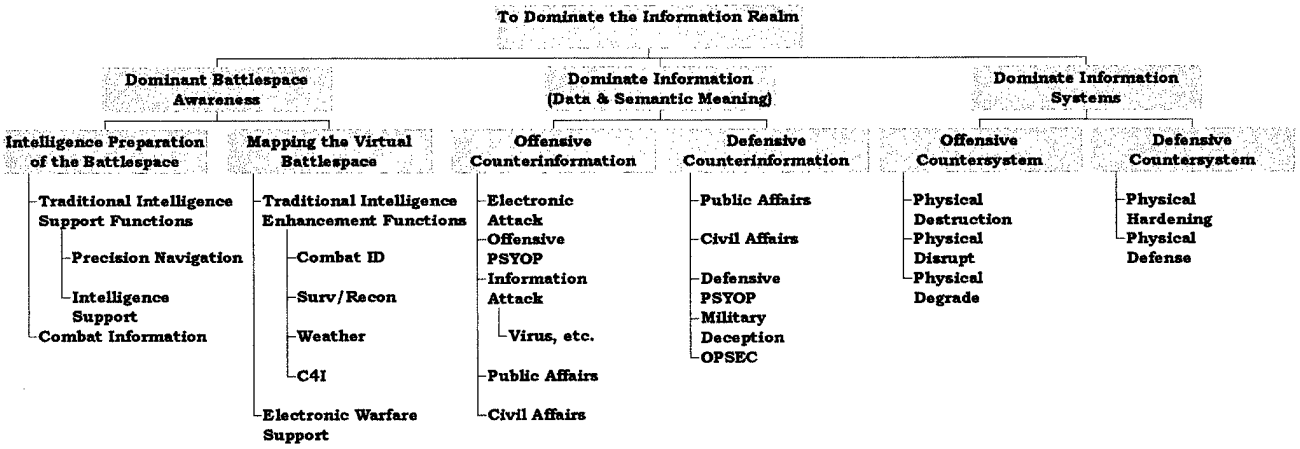

Figure 34: Proposed Value Hierarchy

Table 7: Classification and Testing Criteria

Classification and Testing	
Classifying Definitions	*Objectives*
Information - Data and semantic meaning.	*To Dominate Information* - To make information useless to the adversary while protecting our own information from attack.
Information Systems - Conveyance, storage, or processing that does not add value to the information used by decisionmakers.	*Dominate Information Systems* - To deny, degrade, or alter the adversary's means of data conveyance, storage or non-value added processing while protecting our own from attack.
Information Based Processes - Any process that adds value to information.	*Dominant Battlespace Awareness* - To dominate the adversary's value-adding processes thereby preventing hostile forces from gaining a dominant battlespace awareness while establishing and protecting our own dominant battlespace awareness.

VIII.3. Supporting the Fundamental Objectives

The means objectives for each of these three elements will serve to define each element; narrowing the scope, and leading to action items that can be quantified. Getting to this point will require the input from a cross-section of decisionmakers with the knowledge and experience required to accurately depict the collective values of the US military. Papers and interviews will enable the development of independent attributes that can be used to measure the merit of current and future systems that are intended to be employed in information operations.

The value in conducting this type of analysis stems from the broad value-based development of the objectives. This form of analysis asks "what is needed," not "what can we do with what is handed us." More specifically, by building the requirements from the values of the leadership, the resulting doctrine is prescriptive in nature, and capable of presenting decision opportunities and not simply decision alternatives. Past doctrines have relied on vague, unquantifiable objectives to allow for prescriptive action. A properly constructed value-focused model can provide quantifiable objectives that permit direct merit (value) assessments, and serve to create superior alternatives. From this model, then, will come the measures of merit. More importantly, since this model is prescriptive in nature MOMs can be derived for entire classes or sub-classes of systems that may not exist, thereby, permitting value judgments of new technologies and unrealized alternatives. This, then allows value-based assessments of opportunities for development that are evaluated on a common scale with existing systems. Finally, "holes" on our IO suite of systems can not only be identified based on the values held for IO, but also the value of filling these "holes" can be assessed.

For value-focused thinking, the only meaningful way of completing this process is to include decisionmakers and experts at various levels with various backgrounds to validate and dispute the proposed model, offer new models, weight and score the objectives and attributes, and continually refine the product. In this process it is expected that new, innovative, means and methods will arise; drastically improving the product. To this end, continued efforts are needed, decisionmaker and expert support is needed.

IX. Bibliography

Abraham, Arnold, Air Force Intelligence and Information Warfare, AF/IN White paper, 1 Mar 1996

Date, C. J., An Introduction to Database Systems, 6th ed., Addison-Wesley Pub., 1995

Global Engagement: A Vision for the 21st Century Air Force, http://www.af-future.hq.af.mil/21/coret.inft.htm, downloaded 19 January 1997.

Global Presence, Department of the Air Force, 1995, p. 12.

Griffith, Samuel B., Sun Tzu: The Art of War, Oxford University Press, 1971, P. 41.

Joint Publication 3-13 (Draft), joint doctrine for Information Operations, 21 Jan 1997.

Joint Publication 3-13.1, Joint Doctrine for Command and Control Warfare (C2W), 7 Feb 1996

Joint Vision 2010, OPR Chairman of the Joint Chiefs of Staff, Joint Staff, Pentagon.

Keeney, Ralph, L., Value Focused Thinking: A Path to Creative Decisionmaking, (Cambridge, Mass.: Harvard University Press, 1992).

Parnell, Gregory, Lt Col Jack A Jackson, and LTC Jack M Kloeber, "New Techniques for Value Model Development: Lessons Learned from Major Value-Focused Thinking Studies," presented at the International Conference on Methods & Applications of Multicriteria Decision Making, Mons, Belgium, May 14-16, 1997.

Pinker, A., A. H. Samuel, and R. Batcher, "On Measures of Effectiveness," PHALANX, December 1995, pp. 8-12.

Widnall, Sheila, E. and Ronald R. Fogleman, *Cornerstones of Information Warfare*.

X. GLOSSARY

Command and Control - The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (Joint Pub 1-02) [Joint Pub 3-13: GL-6].

Command and Control Warfare - The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: **a.** C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. **b.** C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system (Joint Pub 1-02) [Joint Pub 3-13: GL-6].

Commander's Estimate of the Situation - A logical process of reasoning by which a commander considers all the circumstances affecting the military situation and arrives at a decision as to a course of action to be taken to accomplish the mission. A commander's estimate which considers a military situation so far in the future as to require major assumptions is called a commander's long-range estimate [Joint Pub 3-13.1: GL-5].

Communications Security (COMSEC) - The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. **a. cryptosecurity**—the component of communications security that results from the provision of technically sound cryptosystems and their proper use. **b. transmission security**—the component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. **c. emission security**—the component of communications security that results form all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. **d. physical security**—the component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents, from access thereto or observation thereof by unauthorized persons. (Joint Pub 1-02) [Joint Pub 3-13: GL-7].

Computer Network Attack - Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. Also called CNA [Joint Pub 3-13: GL-7].

Dominant Battlespace Awareness - Improvements in information and systems integration technologies will also significantly impact future military operations by providing decisionmakers with accurate information in a timely manner. Information technology will improve the ability to see, prioritize, assign, and assess information. The fusion of all-source intelligence with the fluid integration of sensors, platforms, command organizations, and logistics support centers will allow a greater number of operational tasks to be accomplished faster. Advances in computer processing, precise global positioning, and telecommunications will provide the capability to determine accurate locations of friendly and enemy forces, as well as to collect, process, and distribute relevant data to thousands of locations. Forces harnessing the capabilities potentially available from this system of systems will gain dominant battlespace awareness, an interactive "picture" which will yield much more accurate assessments of friendly and enemy operations within the area of interest. Although this will not eliminate the fog of war, dominant battlespace awareness will improve situational awareness, decrease response time, and make the battlespace considerably more transparent to those who achieve it [JV 2010:13].

Electronic Warfare (EW) - Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also Called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. **a. electronic attack**. That division of electronic warfare involved in the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent an enemy" effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). **b. electronic protection**. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from and effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. **c. electronic warfare support**. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and bombing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronic intelligence (Joint Pub 1-02) [Joint Pub 3-13: GL 10].

Information - **1**. Data and the associated semantic meaning required to convey information; a parallel definition to that of a scalar in relational database theory—the smallest "atomic" unit of semantic data; not decomposable without loss of meaning [Date: 81]. **2**. Facts, data, or instructions in any medium or form. Also, the meaning that a human assigns to data by means of the known conventions used in their representation [Joint Pub 3-13: GL-10]. **3**. Facts, data, or instructions in any medium or form [Joint Pub 3-13.1: GL-8]. **4**. Data and the instructions required to give that data meaning [Abraham: 6].

Information Assurance(IA) - Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA [Joint Pub 3-13: GL-10].

Information Operations (IO) - Actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO [Joint Pub 3-13: GL-11].

Information Realm (also Information Environment) - 1. Information is a realm, just as air, space, land, and sea are realms for which militaries strive to dominate. The information realm is that region in which information is collected, processed stored, and transmitted, has its own characteristics of motion, mass, topography, and effect. The information realm is composed of three elements: information, information systems, and information functions [Abraham: 6]. 2. (Information Environment) The aggregate of individuals, organizations, or systems that collect, process, or disseminate information; also included is the information itself [Joint Pub 3-13: GL-10].

Information Superiority - 1. The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same [Joint Pub 3-13: GL-11] and [JV 2010: 16]. 2. That degree of dominance in the information domain which permits the conduct of operations without effective opposition [Joint Pub 3-13.1 GL-8].

Information System - 1. Elements of the information realm that convey, store, or process information without adding value to the decisionmaking processes other than to move the information to the decisionmaking location. 2. The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information [Joint Publication 3-13: GL-11]. 3. The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information [Joint Pub 3-13.1: GL-8]. 4. Any physical component used to acquire, transmit, store, or transform information [Abraham: 6].

Information Warfare - 1. Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries [Joint Pub 3-13: GL-11]. 2. Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks [Joint Pub 3-13.1: GL-9].

Information-Based Processes (also Information Functions) - 1. Any process that adds value to information with respect to decisionmaking processes. 2. (Information Function) The activities involved in the acquisition, transmission, storage, or transformation of information. Within the military, these include surveillance, communications, weather analysis, and others [Abraham: 6]. 3. (Information Function) Any activity involving the acquisition, transmission, storage, or transformation of information [Widnall: 3].

Intelligence Preparation of the Battlespace - 1. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of enemy, environment, and terrain on operations and presents it in graphic form.

Intelligence preparation of the battlespace is a continuing process. Also called IPB (Joint Pub 1-02) [Joint Pub 3-13: GL-12].

Mapping the Battlespace - Real-time awareness of the location, status, and intentions of the adversary, established by penetrating his virtual landscape to include communication networks, nodes, computer technology, and cognitive interaction [Abraham: 11].

Military Deception - Actions executed to deliberately mislead adversary military decisionmakers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: **a. strategic military deception**—Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. **b. operational military deception**—Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater of war to support campaigns and major operations. **c. tactical military deception**—Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. **d. Service military deception**—Military deception planned and executed by the Services that pertain to Service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of Service forces and systems. **e. military deception in support of operations security (OPSEC)**—Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities (Joint Pub 1-02) [Joint Pub 3-13: GL-12].

Operations Security - A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: **a**. Identify those actions that can be observed by adversary intelligence systems. **b**. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. **c**. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC (Joint Pub 1-02) [Joint Pub 3-13: GL-14].

Physical Destruction - Physical Destruction, as an element of C2W refers to the use of "hard kill" weapons against designated targets as an element of an integrated C2W effort. Although the word "destruction" is used in the term, "hard kill" weapons may be used in C2W for a purpose other than the actual destruction of a specific target. Firepower demonstrations or selective degradation of certain parts of a C2-related target through weapons effects are examples of the use of "hard kill" weapons for a purpose other than actual destruction that might be part of an integrated C2W plan. Normally, physical destruction would target identified C2 nodes. However, physical destruction may also be against targets other than adversary C2 nodes in support of one or more of the other elements of C2W.

Psychological Operations - Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called **PSYOP** (Joint Pub 1-02) [Joint Pub 3-13: GL-14].

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	July 1997	Technical Report

4. TITLE AND SUBTITLE

A Value Function Approach to Information Operations MOE's: A Preliminary Study

5. FUNDING NUMBERS

6. AUTHOR(S)

Capt Michael P. Doyle, USAF; Dr. Richard F. Deckro;
LTC Jack M. Kloeber Jr., USA; Lt Col Jack A. Jackson Jr., USAF

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

Air Force Institute of Technology
2750 P Street
WPAFB OH 45433-6583

8. PERFORMING ORGANIZATION REPORT NUMBER

CMSATR/97-04

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

Department of Energy/EM-50

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

A value-focused thinking approach is applied to information operations. A preliminary value hierarchy for information operations is constructed by extracting the values of senior military leadership from existing doctrine. To identify these key values for information operations, applicable existing doctrine was reviewed and summarized. Additionally, hierarchical representations of the values represented within each reviewed doctrine are developed. A value hierarchy requires that supporting objectives be mutually exclusive and collectively exhaustive. Within this analysis, these requirements are enforced, in part, by developed definitions which serve as tests to maintain mutual exclusivity. An exhaustive set of supporting values is also guaranteed by identifying a spanning set of values that directly support the overall objective of information operations. This preliminary value hierarchy serves as the basis for continuing research. The implications for this research include the construction of a prescriptive model in which the effectiveness of current and future systems can be assessed on a common scale. Further, the effectiveness of developing technologies can be assessed and the value of these technologies determined with respect to the values of senior military leadership. With this, the value of "holes" in our suite of information warfare systems can also be assessed in terms of their effectiveness in fulfilling the values of military leadership.

14. SUBJECT TERMS	15. NUMBER OF PAGES
decisionmaker, value-focused thinking, information warfare	58
	16. PRICE CODE

17. SECURITY CLASSIFICATION	18. SECURITY CLASSIFICATION	19. SECURITY CLASSIFICATION	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified GE	Unclassified T	UL