AIR LAND SEA APPLICATION CENTER

Information Warfare/Information Operations Study

15 December 1995

ALSA Information Warfare/Information Operations (IW/IO) Study
Contents

INFORMATION WARFARE/INFORMATION OPERATIONS STUDY

Air Land Sea Application Center (ALSA), Langley AFB, VA

15 December 1995

1. Overview

In June, 1995, the Joint Action Steering Committee (JASC) tasked the Air Land Sea Application (ALSA) Center to conduct a study on Information Warfare / Information Operations (IW/IO). This study was initiated to support the Department of the Army Deputy Chief of Staff for Operations, Future Developments Branch tasking to TRADOC-DCSCD for an Information Operations CBRS (Concept Based Requirement System) assessment. The purpose of this study is to provide TRADOC-DCSCD and the JASC an unbiased, objective perspective of the primary issues involved in the development of IW/IO doctrine, highlighting areas of consensus or divergence of opinion, and to identify the principle individuals/organizations responsible for IW/IO doctrinal development within the Services. Recommendations for standardizing the doctrinal development of Information Warfare are beyond the scope of this study.

DoD is still in the process of defining and articulating its position on Information Warfare issues. Consequently, the Services are in a state of transition in IW doctrine development. Because of the transitory nature of the subject area, the majority of the research conducted for this study is time-sensitive. Many of the Service documents addressing IW are currently in draft stages, with the Services refining their positions on IW on a continuous basis. Therefore, the findings of this study should be considered a snapshot in time within a very fluid environment.

ALSA began this study by reviewing joint and Service specific documents concerning IW/IO and interviewing Service representatives with responsibility for developing IW

doctrine. This research led to participation at the Land Information Warfare Activities (LIWA) and Association of Old Crows Information Warfare symposium at McLean, Virginia in October 1995. During this symposium, representatives from the Services presented their views on IW issues, and addressed how their specific Service is approaching doctrinal development in the area of Information Warfare. This study presents the research data in four major subject areas: joint IW/C2W guidance, specific Service IW perspectives, comparison of Service perspectives, and common Service challenges.

2. Joint Information Warfare (IW) / Command and Control Warfare (C2W) Guidance

A significant challenge facing the Services as they develop IW policy and doctrine is the fact that DoD is in the midst of developing the guidance that defines the military's roles and responsibilities in Information Warfare. In addition, the complete realm of IW is still relatively new to DoD, and comprehensive, specific guidance is not yet available to the Services.

a. Information Warfare

(1) DoD Directive S-3600.1 (draft) will be the key directive for the implementation of IW policy. This directive, when signed, will task the Services to organize, train, and equip to achieve information superiority (defined as that degree of dominance in the information domain which permits the conduct of operations without effective opposition)[1] over potential adversaries in order to facilitate the ability to win quickly and decisively, with minimum loss and collateral effects. It recognizes IW as an integrating strategy based on the need for and use of information throughout the spectrum of conflict.

[1] Working definition proposed by ASD (C3I) in DoD Directive S-3600.1 (draft)

(2) DoD recognizes the impact information has on today's military. As the United States approaches Toffler's "third wave" status, we become more and more reliant on the acquisition and transfer of information. By emphasizing the integration of IW into military strategies, DoD Directive S-3600.1 (draft) tasks the Services to consider IW implications when defining and validating requirements, conducting research and development, acquiring systems, and planning and conducting operations. Additionally, it defines the need to "vigorously" pursue information system defensive measures to preclude potential adversary attacks against DoD information and information systems.

(3) DoD Directive S-3600.1 (draft) also dictates that IW policies and plans be integrated with overall national security objectives. To facilitate this, the directive outlines IW responsibilities from the level of the Deputy Secretary of Defense through the Chairman of the Joint Chiefs of Staff. Under this guidance, primary responsibility for the development of IW policy belongs to the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD(C3I)), whose key charter is to develop, coordinate, and oversee the implementation of DoD policy on Information Warfare. (Reference Annex A)

b. Command and Control Warfare (C2W)

(1) CJCS Memorandum of Policy (MOP) 30, 8 March 93, provides the primary joint policy and guidance for C2W. MOP 30 defines the goal of C2W as the capability to enable the friendly commander to seize the initiative by forcing the enemy into a reactive mode, while maintaining, protecting, and/or enhancing the effectiveness of friendly command and control. It describes the goals of denial and influence of adversary information, through deception, disruption, and destruction of adversary command and control while simultaneously protecting friendly capabilities. To achieve these goals, MOP 30 calls for the integration and synchronization of five principal military actions: operations security (OPSEC), psychological operations (PSYOP), military deception, electronic warfare (EW), and physical destruction, all

mutually supported by intelligence. These principal military actions are commonly referred to throughout DoD as the five elements of C2W.

(2) The military has performed these five elements for years. MOP 30's emphasis on C2W outlines the synchronization and orchestration of these elements to achieve a synergistic effect on the battlefield. Each of the elements can produce measurable effects if performed independently; however, combat power is maximized through the synergistic application of all five elements. It is this integrated employment that is the essence of the MOP 30 C2W strategy: an efficient, effective, coordinated application of different capabilities, processes, techniques, and weapons across the organizational spectrum of an adversary's command and control system.

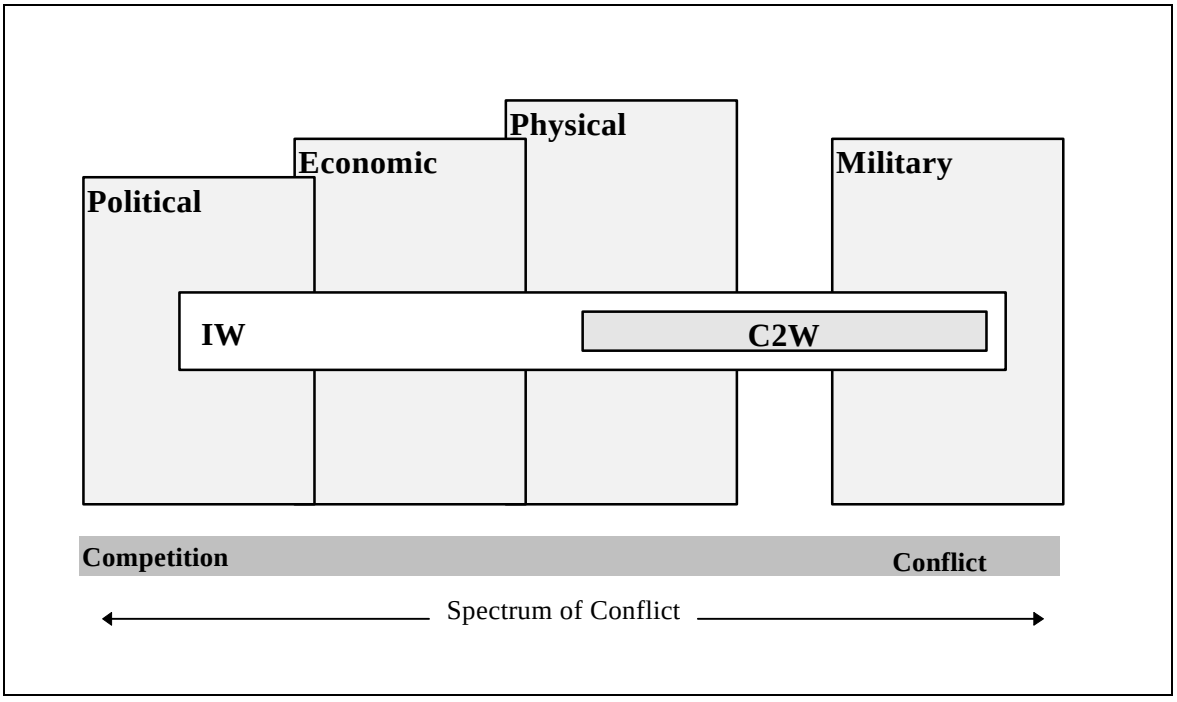
(3) Unlike DoD Directive S-3600.1 (draft), MOP 30 contains fairly specific guidance on the execution of C2W. It delineates the roles of intelligence and counterintelligence in support of C2W, as well as the general support intelligence must provide. Additionally, MOP 30 provides guidance on communications support, joint frequency spectrum management, C2W planning and execution concepts, validation of equipment, tactics, and procedures, training, and considerations for coordinating with our allies. Building on the MOP 30 guidance, Joint Publication 3-13, *Joint Doctrine for Command and Control Warfare* (draft), expands and amplifies guidance for a C2W strategy.

(4) MOP 30 is currently under revision. The latest version contains a statement which seems to have led to some Service disparity. MOP 30 states that "C2W is <u>the</u> military strategy that implements Information Warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from the body of its forces."[2] This definition, when taken in its purest form, has been interpreted by many to imply that the military's role in the amorphous realm of IW is limited to the constructs of C2W. This interpretation has

[2] Chairman of the Joint Chiefs of Staff Memorandum of Policy Number 30, 17 July 1990 (1st revision 8 March 1993), pg. 3

subsequently led to variances in Service approaches to answer the DoD Directive S-3600.1 (draft) tasking to "organize, train, and equip" for IW.

(5) Some of the confusion is being resolved through the revision of definitions and new guidance. The latest directives from ASD(C3I), as of 15 Sep 95, define IW as "actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems."[3] When combined with the guidance proposed in Joint Publication 3-13 (draft), the relationship of IW and C2W begins to appear (Figure 1). The final draft of Joint Pub 3-13 states that "C2W is *a* warfighting application of Information Warfare in military operations and is a subset of IW. C2W employs various techniques and technologies to attack or protect a specific target set - C2."[4]



[3] Definition signed out by ASD (C3I) 15 September 1995, presented at Joint Doctrine Working Party, Ft Monroe, VA., 24 October 1995

[4] Definition proposed in final draft of Joint Pub 3-13, Joint Doctrine for Command and Control Warfare (C2W), presented at the Joint Doctrine Working Party, Ft Monroe, VA., 24 October 1995

Figure 1. IW/C2W Relationship[5]

(6) Further clarification of IW and C2W constructs should be provided through Chairman of the Joint Chiefs of Staff Instruction (CJCSI)-3210, "Joint Information Warfare Policy", which is currently in draft. This document will provide the Chairman of the Joint Chiefs of Staff's policy and guidance on IW, and will lay the foundation for the development of joint IW doctrine. When published, CJCSI-3210 will discuss the role of IW in Military Operations Other Than War (MOOTW) and other scenarios. It will include policy guidance on military offensive and defensive IW capabilities, intelligence support to IW activities, technology development, IW training and education, and legal considerations involved in IW planning. Enclosures to the document will include the IW responsibilities for the CINCs, Services, Defense Agencies, and the Joint Staff, detailed description of a CINC/JTF IW cell, and considerations for offensive IW planning and execution.

c. **Joint Organizational Hierarchy:** Key departments within DoD and the Joint Staff and their primary responsibilities in the IW realm are listed below.

(1) ASD(C3I): Develops, coordinates, and oversees implementation of policy on IW matters. Principal staff assistant and advisor to the Secretary of Defense for DoD IW activities.

(2) Information Warfare Executive Board (IWEB): The IWEB is a DoD working group to address IW planning, policy, and legal issues. The board was established and is chaired by the Deputy Secretary of Defense. Membership includes the VCJCS, the Vice Chiefs of the Services, the Deputy Director for Counter Intelligence, the NSA Director, the DIA Director, Under Secretary of Defense for Policy, Under Secretary of Defense for Acquisition and Technology, Comptroller,

[5] Rowe, Wayne J. Strategic Research Department of the Center for Naval Warfare Studies, Information Warfare: A Primer for Navy Personnel, June, 1995

General Counsel, Director DISA, NSC representatives, and ASD(C3I). The IWEB is briefed on IW issues, participates in wargames which incorporate IW activities, addresses IW roles and responsibilities, and serves as the DoD focal point for IW discussion at the National level.

(3) Office of Net Assessment (OSD/NA): The Director of OSD/NA provides long term analytical support to the SECDEF, and when the SECDEF directs, to other senior officials in DoD (Under Secretary of Defense for Policy, Under Secretary of Defense for Acquisition and Technology, CJCS, and the CINCs) on issues and trends in military affairs of potential importance for DoD. Several years ago, DoD identified IW as a potentially important new warfare area; therefore, IW has been the subject of a widely ranging study effort within OSD/NA ever since.

(4) Defense Information Systems Agency (DISA): Central manager of the Defense Information Infrastructure (DII). As such, DISA has the responsibility to "in consultation with the Directors of the Defense Intelligence Agency and the National Security Agency,provide technology and services to ensure the availability, reliability and maintainability, integrity, and security of defense information."[6] In general, the DoD C2 protection actions associated with IW/C2W are managed by DISA, but are implemented by the Services.

(5) Secretaries of the Military Departments: Develop IW doctrine and tactics, and organize, equip, and train their departments to ensure IW becomes an essential element of U.S. military capabilities.

(6) Joint Staff: J-38 is responsible for all offensive IW programs and activities coordinated by the joint staff, while J6K is responsible for all defensive IW programs and activities. The two divisions fully share responsibility for all aspects of broad policy, assessment, and doctrine.

---

[6] DoD Directive 8000.1, Defense Information Management Program, 27 October 1992

(7) Joint Command and Control Warfare Center (JC2WC): The JC2WC is the principal field agency within DoD for non-Service specific C2W support. They provide direct C2W support to operational commanders and support the integration of the five elements of C2W throughout the planning and execution phases of operations. This direct support is provided to joint force commanders, Service component commanders, and functional component commanders through geographically oriented augmentation teams. The JC2WC also supports OSD, the Joint Staff, U.S. government agencies, NATO, and allied nations as directed. This organization is the DoD focal point for identifying, and coordinating access to, those data bases/data and information systems necessary to establish a common joint information base for conducting C2W. As the Joint Center for Excellence in C2W operations, they maintain responsibility for joint C2W doctrine development, development and maintenance of C2W decision aids, and modeling and simulation tools.

(8) Joint COMSEC Monitoring Activity (JCMA): Conducts COMSEC collection, monitoring, and reporting of DoD telecommunications and automated information systems, to identify vulnerabilities exploitable by potential adversaries and to recommend countermeasures. JCMA's primary support is to the CINCs, subordinate component commanders, DoD agencies, and the Joint Staff. JCMA does not routinely perform "traditional" telephone monitoring. This is the responsibility of Service Cryptological Elements (SCEs). However, if given Executive Agent authority, JCMA will coordinate with SCEs to ensure complete support to the requesting agency.[7]

3. Service Perspectives

a. Army Information Operations Doctrine

[7] Science Applications International Corporation (SAIC), Information Warfare - Legal, Regulatory, Policy, and Organizational Considerations for Assurance, 4 July 1995, pp. A-6 - A-15

(1) The Army's approach to IW policy and doctrine centers on their Information Operations (IO) concept. The Army defines IO as "Continuous military operations within the Military Information Environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. Information Operations include interacting with the Global Information Environment and, as required, exploiting or denying an adversary's information and decision systems."[8] The Army decided to develop IO vice IW/C2W for two primary reasons.

(a) First, the Army is firmly engaged in planning for the future. The digitized battlefield is the linchpin of the Army's Force XXI vision, allowing seamless C2 from the Corps commander to the soldier in the foxhole. Inherent in this vision is the need to gain and maintain information dominance, which gives Army commanders the ability to access the information required to coordinate and synchronize battlefield actions. MOP 30 acknowledges that the military has become heavily reliant on information and information systems. Moreover, as the military's reliance on information increases, the vulnerability to an information attack waged by potential adversaries increases as well. To account for this vulnerability, DoD is challenging the Services to minimize the amount of information transfer required for effective command and control of U.S. forces to enable successful operations in a possibly degraded information and communication environment.[9] However, advances in precision guided munitions and smart weapon technology have forced the Army commander to disperse his forces over the battlefield for survivability. The need exists to develop information systems and command and control procedures that allow the commander to visualize and control the expanded battlefield. Instead of minimizing information transfer requirements, the Army sees the need for

[8] TRADOC Pamphlet 525-69, Concept for Information Operations, 1 August 1995
[9] DoD Directive S-3600.1 (draft)

increased information transfer requirements. Therefore, IO includes an integrated emphasis on information systems and their protection.

(b) Secondly, the Army feels that the term Information Warfare is too restrictive. Using the term *warfare* implies that IW is restricted to combat operations. The Army developed the IO concept to recognize the fact that information permeates the full range of military operations, beyond just the traditional context of warfare, from peace through global warfare. In the Army's view, the need to affect the flow of information extends beyond the traditional battlefield, and involves more than targeting the adversary's information systems while protecting our own. It also requires awareness and sensitivity to non-military information sources that can ultimately impact the overall campaign. Therefore, IO expands the commander's battlespace, and includes worldwide interaction with the media, industry, joint forces, multinational forces, and computer networks.[10]

(2) Information Operations are built around three primary components: C2W, information systems, and intelligence.[11] Much of the IO concept is consistent with joint doctrine. The exploitation and denial of the adversary's information system and the protection of friendly capabilities is called C2W and encompasses the five primary elements of EW, OPSEC, military deception, PSYOP, and physical destruction. C2W is both offensive and defensive and is categorically defined as C2-attack and C2-protect. Each category integrates the five C2W elements with intelligence support. However, Army IO adds information systems (to include battle command and interaction with the global information) and intelligence operations to the joint C2W foundation in order to clarify the scope of IO.

(3) All of the Army's current policy and doctrine for IO reflect the boundaries established by previous definitions of IW and C2W [see paragraph 2.b.(4)]. AR 525-20 (Information Warfare/Command and Control Warfare Policy [draft]), TRADOC

---

[10]FM 100-6, Information Operations, Final Draft, 13 November 1995
[11] ibid.

Pamphlet 525-69 (Concept for Information Operations), and the final draft of FM 100-6, the capstone doctrine for Information Operations, refer to C2W as the warfighting application of IW in military operations. Therefore, the majority of the Army's "traditional" IW application can be distilled to C2W.

(4) FM 100-6 breaks C2W down into the primary categories of C2-attack and C2-protect, which is consistent with the categorization in Joint Pub 3-13 (draft). The goal of C2-attack is to prevent an adversary from exercising effective command and control over his forces. In combat situations, C2-attack can strike at all echelons, targeting personnel, equipment, communications, and/or facilities to disrupt or shape the adversary's battlefield awareness. In non-combat situations, the goal of C2-attack is to control the flow of information and situational awareness. Throughout the spectrum of conflict, the commander has several C2-attack options, ranging from denying the enemy information to influencing, degrading, or destroying the adversary's C2 system.

(5) C2-protect seeks to maintain effective C2 of friendly forces by negating the adversary's attempts to influence, degrade, or destroy friendly C2 systems. C2-protect also considers countering an adversary's propaganda strategy to prevent it from affecting friendly operations, options, public opinion, and the morale of friendly troops. It starts with the need to gain and maintain command and control superiority. C2 superiority includes unimpeded friendly processing of information, accurate development of courses of action, valid decision making, and effective communication throughout the chain of command. C2-protect maintains the friendly capability to stay inside the adversary's decision cycle. Finally, it reduces the adversary's ability to conduct C2-attack, reduces friendly C2 vulnerabilities, and reduces friendly interference within C2 systems by coordinating and deconflicting the use of the electromagnetic spectrum.

(6) The Army is cognizant of the threat to friendly information systems. These systems continue to face traditional threats such as SIGINT exploitation, electronic attack, and physical destruction. However, the proliferation of globally networked

systems opens the possibility for new vulnerabilities, such as computer intrusions and the insertion of malicious software. The Army chose to base much of its C2-protect strategy on the concept of risk management versus risk avoidance. The IO concept acknowledges the fact that it is infeasible to prevent all breaches of security within Army and DoD information systems.[12] Therefore, the Army is concentrating on various protection measures that will minimize the damage if an adversary penetrates a system.

(7) While the Army emphasizes the impact information has on military operations, they do not view the attainment of "perfect knowledge" as the ultimate end-state in a campaign. IO is a supporting strategy to facilitate the conduct of operations as outlined in FM 100-5. In their view, achieving superior relative combat power against an enemy, or establishing situational dominance in operations other than war, remains the primary military objective.[13]

(8) Organizational Hierarchy

(a) At the Army Staff level, there are four key elements performing IW activities: Assistant Secretary of the Army (Research/Development/Acquisition) (SARDA); Office of the Deputy Chief of Staff for Operations and Plans (ODCSOPS); Office of the Deputy Chief of Staff for Intelligence (ODCSINT); and Office of the Deputy Chief of Staff for Information Systems, Communications, Computers, Command and Control (ODISC4). Also, as previously mentioned, the Army Digitization Office's Force XXI project is involved in IO development.

(b) At the Army MACOM level, the following organizations are involved in IO development and activities: Intelligence and Security Command (INSCOM), Ft. Belvoir; Information Systems Command (ISC), Ft. Huachuca; Training and Doctrine Command (TRADOC), Ft. Monroe, and the Army supported CINCs.

---

[12] FM 100-6, Information Operations, Final Draft, 13 November 1995
[13] ibid.

(c) The primary OPRs for the IO concept fall under ODCSOPS. The Deputy Chief of Staff for Operations Future Developments branch (DCSOPS-FD) is playing a key role in the development of Information Operations. The Land Information Warfare Activity (LIWA), supervised by DCSOPS-OD, was established in the fall of 1994. LIWA provides operational IW/C2W support to field commanders through Field Support Teams (FSTs). Additionally, LIWA provides the Army with Red Team IW assistance for field training exercises and Computer Emergency Response Teams (CERTs).[14]

b. Air Force Information Warfare Doctrine

(1) The Air Force is changing its basic doctrine to emphasize the impact of information in today's environment. The former strategy of "Global Reach, Global Power" has been revised to "Global Reach, Global Power, and Global Awareness." The Air Force recognizes the dimension of information as a distinct medium, equal to air, land and sea, within which the military may wage war.[15] Two statements in the draft version of Air Force Doctrine Document 1 (AFDD-1) summarize the Air Force's view of IW. First, AFDD-1 (draft) states that "Air and space power is no longer just aircraft and satellites, but information power as well." It also states that "Air and space power (*which includes information power*) is best applied as a strategic force." These statements highlight the fact that the Air Force has subsumed IW into its long standing strategic approach to warfare.

(2) AFDD-1 (draft) states six basic roles for the Air Force: Control; Strike; Mobility; Information; Sustainment; and Preparation. Of these six, the Control, Strike, and Information roles directly reflect USAF IW doctrine.

(a) *Control: Actions taken to attain freedom of operations in the air, space, and information environments. History has proven time and again that attaining*

[14] SAIC, pp. A-19 - A-20
[15] USAF Concept Paper, Cornerstones of Information Warfare, pg. 2

control of the operating environment is the first priority of air and space forces and necessary to performing all other roles and missions in time of war.

(b) *Strike: An attack from the air, space, or information environments intended to inflict damage or affect the enemy's operations and attain strategic, operational, and/or tactical objectives.*

(c) *Information: Information missions enhance the employment of air and space forces. Space systems, intelligence, and communications are crucial to these operations, enhancing the precision, lethality, and agility of warfighting forces, and enhancing a commander's opportunity to succeed across the range of military options.*[16]

(3) The Air Force definition of IW is similar to the definition in Joint Pub 3-13 (draft) [see paragraph 2.b.(5)]. "Information Warfare: Any action to deny, exploit, corrupt, or destroy information and its functions; protecting ourselves against those actions; and exploiting our own information functions."[17] As with the other Services, the Air Force uses some unique definitions and terminology to define its IW doctrine. An information function is defined as "any activity involving the acquisition, transmission, storage, or transformation of information."[18] The Air Force's vision of IW consists of targeting the enemy's information and information functions, while protecting friendly capabilities, with the intent of degrading his will and capability to fight. They subsequently use this approach as the basis for several key assertions:

(a) Information Warfare is any attack against an enemy information function, regardless of the means. Bombing a communication switching facility is IW, just as destroying the facility's control software is IW.

(b) Information Warfare is any action taken to protect a friendly information function, regardless of the means. Therefore, hardening and defending the

---

[16] AFDD-1 (Draft)
[17] Cornerstones of Information Warfare, pg. 3
[18] ibid.

switching facility against attack, and using an anti-virus program to protect the software are both examples of IW.

(c) Information Warfare is a means, not an end, in precisely the same manner that air warfare is a means, not an end. IW can be used as a means to conduct interdiction or strategic attack missions, just as air power can be used for interdiction or strategic attack missions.[19]

(4) The Air Force includes six primary elements within the construct of IW: Psychological Operations, Electronic Warfare, Military Deception, Physical Attack, Operations Security, and Information Attack. The first five elements are consistent with joint guidance outlined in MOP 30 and Joint Pub 3-13 (draft) for C2W. The Air Force has expanded the horizon with the addition of Information Attack, which is defined as "directly corrupting information without visibly changing the physical entity within which it resides."[20] For example, a SOF team placing a powerful magnet on a hard disk is a form of information attack. The inclusion of information attack supports a breakout of direct and indirect applications of IW. Indirect IW affects information by creating conditions that the adversary perceive, interpret, and act upon. Military deception, physical attack, OPSEC, EW, and PSYOP traditionally fall into indirect applications of IW. Direct IW with information attack affects information without relying on the need to affect the adversary's interpretations or perceptions.

(5) As previously stated, the Air Force views information as an intrinsic element in air power. There are three primary objectives of air warfare: control the air while protecting friendly forces from enemy action; strike enemy capabilities in order to affect their will and capacity to fight; enhance overall force effectiveness. Similarly, there are three primary objectives of Information Warfare: control the information realm so we can exploit it while protecting our own information functions from

---

[19] ibid.
[20] Cornerstones of Information Warfare, pg. 6

enemy action; strike the enemy's information and information functions in order to affect their will and capacity to operate; enhance overall force effectiveness by fully developing information functions.

(6) To provide consistency with standing air doctrine, the Air Force has used parallel terminology to define the missions inherent with IW. Under the first objective of controlling the information realm, the Air Force defines the mission of counter-information (CI), which parallels the counter-air mission. CI has two subsets: offensive counter-information and defensive counter-information. Offensive counter-information enables us to use the information realm and impedes the adversary's use of the information realm. Defensive counter-information includes both active and passive measures to protect ourselves from the adversary's IW actions.

(7) Once control of the information realm has been achieved, missions to strike the information and information systems can begin. Since the Air Force stresses that IW is a means to accomplish an objective, they feel IW can be used to conduct strategic attack, interdiction, or any other traditional mission. C2W is viewed as just one application of IW. With this view, C2W only addresses activities directed against the adversary's ability to direct the disposition and employment of forces, or those which protect the friendly commander's C2 capabilities. Therefore, C2W is only a discrete application of IW for the Air Force.

(8) The third objective is to enhance total force effectiveness. Examples of information missions that enhance force effectiveness include surveillance, reconnaissance, command and control, communications, intelligence, precision navigation aids, and weather support.[21]

(9) Organizational Hierarchy. The Air Force is currently conducting a review to delineate IW responsibilities.

---

[21] Air Force Doctrine Document 1 (draft), Air Force Basic Doctrine, 1 August 1995

(a) The Assistant Chief of Staff for Intelligence (ACSI) is responsible for performing those intelligence functions related to IW.

(b) The Air Intelligence Agency and the Air Force C4 Agency are charged with developing Air Force security programs. In addition, AIA acts as facilitators for resolving IW issues or requirements. AIA/XRXI is responsible for information operation issues and defensive issues.

(c) Air Force XOXD and XOXT are responsible for developing IW policy.

(d) The Air Force Doctrine Center is developing AFDD-1 (Basic Doctrine) and AFDD-5 (Information Warfare Doctrine).

(e) The Air Force Information Warfare Center (AFIWC) closely resembles LIWA in application. As the Air Force Center of Excellence for IW issues, AFIWC has the following responsibilities: organize, train, equip, and deploy IW/C2W support teams to augment JFACC/AOC and CINC/JTF staffs; build and maintain C2W data bases, and modeling and simulation applications; analyze the vulnerabilities and capabilities of friendly electronic systems; protect friendly information and information systems against adversary attacks; integrate special capabilities, techniques, and tactics to support the operational commander's campaign plan.[22]

c. Navy Information Warfare Doctrine

(1) In many aspects, the Navy's approach to IW closely resembles that of the Air Force. The Navy has fully embraced the concept of IW, and is folding it into their "Forward... From the Sea" doctrine. Just as Air Doctrine does, the Navy recognizes the break between C2W and IW. Due to their constant forward presence, the Navy feels particularly suited for projecting both IW and C2W across the spectrum of conflict with minimum response time. In a recent speech, the Chief of Naval Operations, Admiral Boorda, stated: "Because our posture forward allows the Navy

[22] AFIWC presentation given at AOC/LIWA IW symposium, 25 October 1995

to be in position when crises develop, Information Warfare will give us the ability to slow and influence the enemy's decision making cycle, to prepare the battlespace before the start of hostilities, and to dictate the battle on our terms."[23] However, just as with the other Services, the Navy is currently in a transitional state of defining the requirements, organizational structures, and policies necessary to fulfill this capability.

(2) The most current naval guidance is OPNAVINST 3430.26, which issues implementation guidance and organizational relationships for IW/C2W. This document defines IW as "the action taken in support of national security strategy to seize and maintain a decisive advantage by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems. C2W is the action taken by the military commander to realize the practical effects of IW on the battlefield."[24] This definition is a prime example of the transitory state of IW doctrinal development. While the definition implies that the Navy views C2W as the military's role in IW (similar to the Army's C2W portion of IO), current doctrine is evolving that delineates C2W as a specific subset of IW. The Navy acknowledges that they may be tasked to perform missions that do not fall within the traditional boundaries of C2W, as does the Air Force.

(3) The Navy has been involved with OPSEC, deception, destruction, and electronic warfare for years. An integral part of the Composite Warfare Commander (CWC) concept is the C2W Commander (C2WC), who has the responsibility for orchestrating and executing the Battle Group Commander's C2W plan.[25] NDP 3-13.1 (draft) is being developed to provide guidance for the C2WC. The Navy's C2W approach appears to be consistent with joint guidance; however, they substitute the term counter-C2 for the joint term C2-attack.

---

[23] Admiral J.M. Boorda, Chief of Naval Operations, taken from a speech given 23 March 1995 to AFCEA
[24] OPNAVINST 3430.26, 18 January 1995, page 1
[25] Armed Forces Staff College, Joint Command and Control Warfare Staff Officer Course Student Text, April 1995, page 17-8

(4) With respect to IW, the Navy is pursuing the capability to achieve strategic, operational, and tactical effects on the battlefield. Current guidance lists the standard five elements identified in MOP 30 as the elements comprising IW as well as C2W. The Navy feels that C2W as a concept is too restrictive. While the C2W elements identified in MOP 30 may be used as tools, target sets may fall outside the bounds of affecting the adversary's command and control capabilities.

(5) While the Navy is vigorously pursuing the development of C2W and IW capabilities, they are currently not as far along as the Army or the Air Force in documentation that supports their IW doctrine. Their near term goal is to identify the requirements necessary to support operational commanders, primarily, the Fleet Commander. Once those requirements are identified, the Navy intends to pursue the tactics and techniques to meet the requirements, and develop the doctrine for implementation.

(6) Organizational Hierarchy:

(a) Deputy Chief of Naval Operations (DCNO) (Plans, Policy and Operations) (N3/N5) is responsible for the development of Service IW/C2W policy, strategy, and operational concepts and for coordination with the Joint Staff.

(b) Director Space, Command Control, and Information Warfare (N6) is responsible for overall IW/C2W development and implementation guidance. N6 serves as the cross platform IW/C2W resource sponsor and is the working level POC for IW in the Navy. Within N6, N64 is responsible for IW/C2W.

(c) Deputy Chief of Naval Operations (DCNO) (Resources, Warfare Requirements and Assessments) (N8) is the resource sponsor for single platform IW/C2W systems.

(d) Director of Naval Intelligence (N2) is the focal point for intelligence and threat support to Navy-related IW/C2W program efforts. N2 coordinates with National

agencies/organizations for satisfaction of Navy IW/C2W intelligence requirements.

(e) Chief of Naval Education and Training (CNET) is responsible for the development of Naval and Joint schoolhouse IW/C2W training and education in support of Naval, Joint, and Combined IW/C2W doctrine.

(f) Commander, Naval Security Group (COMNAVSECGRU) serves as the CNO's executive agent for IW/C2W training, manpower, and equipment requirements. The seat of the Navy's Cryptologic Community, they have the requisite technological expertise and experience to develop and field Naval IW capabilities.

(g) Naval Information Warfare Activity (NIWA) is the CNO's principal technical agent and interface to Service and national level agencies engaged in the pursuit of IW/C2W technologies. NIWA develops the tools of the trade for Naval IW.

(h) Fleet Information Warfare Center (FIWC) is the Navy's Center of Excellence for IW. FIWC is the Fleet CINC's principal agent for development of IW/C2W tactics, procedures, and training. They deploy trained personnel with offensive and defensive IW systems. NIWA and FIWC work closely together to develop and field Naval IW capabilities.[26]

d. United States Marine Corps Information Warfare Doctrine

(1) The Marine Corps approach to IW/C2W results from two major service philosophies, operational focus and Naval character. First, the Marine Corps is an operational force. Tactics, doctrine, and procedures are designed to allow them to win quickly and decisively on the operational and tactical battlefield. The USMC views C2W as those actions taken by military commanders to realize the practical effects of IW on the battlefield. This view is particularly well suited to complement other Marine Corps concepts of maneuver warfare and "Forward... From the Sea."

[26] OPNAVINST 3430.26, interview with N64

Therefore, the Marine Corps has focused its efforts on C2W, and on integrating C2W into all operational plans.

(2) The USMC is in alignment with the terminology and elements of C2W outlined in Joint Pub 3-13 (draft). Although they may not be directly involved with executing each of the elements in a campaign, they plan on integrating and synchronizing their capabilities and augmenting other C2W actions, to support the operational commander's concept of operations. The USMC has always planned the use of the five C2W elements, but they have also recognized that due to increased reliance on information and information systems, closely coordinating the use of the elements can produce a synergistic effect never previously achieved.

(3) The second aspect that impacts on USMC IW/C2W is their close ties with the Navy and Naval operations. USMC planning and concepts for the employment of C2W are closely connected and coordinated with their Navy counterparts. As Naval Expeditionary Forces are tasked with a mission, C2W planning must provide for a smooth transition from sea-based operations to shore-based operations. Therefore, USMC C2W must be in consonance with the Navy's view as well. There are unique aspects to each Service's organization and philosophy for C2W, but the essential elements of planning and execution are the same.

(4) Like the Joint Staff, the Marines view C2W as a coordinating strategy rather than a warfare function. As such, there will not be any major changes to their current doctrine. However, they are currently developing, in coordination with the Naval Doctrine Command, an overarching document which will build the framework for the coordination and execution of the five C2W elements. Also, the doctrinal pubs covering the five elements are being rewritten to ensure the synergistic effects of combining their application are emphasized.

(5) This is not to say the USMC is ignoring IW, or its implications. Clearly there are aspects of IW, not explicitly included in C2W, that could be used at the operational

and tactical levels. Those aspects, such as Civil Affairs, will be integrated into their operational plans as the need arises.

(6) The USMC plans for the use of IW capabilities within the normal Joint coordination channels, although they do not typically develop their own systems. Most of these capabilities, however, require significant lead time for their employment, which is not conducive to rapid response-type missions for which the Marine Corps is generally tasked. In addition, a significant portion of IW is focused at the strategic and national level, which the USMC is not designed to support.

(7) The one area of IW in which the USMC places great emphasis is the defense. Major efforts are underway to protect their information systems, both garrison and tactical. These efforts include, but are not limited to, general awareness training, developing more robust INFOSEC procedures, and the placement of "firewalls" and other anti-intrusion devices on the systems themselves. The USMC is committed to providing forces to the Joint commander that are trained and equipped for IW, specifically C2W.

(8) Organizational Hierarchy:

(a) Headquarters, U.S. Marine Corps (HQMC), Plans, Policy, and Operations (PP&O) has direct responsibility for providing overall IW/C2W policy and guidance.

(b) HQMC Command, Control, Communications, Computers, and Intelligence (C4I) is responsible for all intelligence, counter-intelligence, and information security aspects of IW/C2W. They also conduct vulnerability assessments of USMC systems to sabotage and other forms of attack.

(c) HQMC Aviation is responsible for all aviation aspects of IW/C2W.

(d) HQMC Programs and Resources (P&R) is responsible for supervising the programming activities for all IW/C2W related items.

(e) The Marine Corps Combat Development Command (MCCDC) is responsible for developing concepts, doctrine, training, and other related items to support the operational forces in executing C2W. They also conduct Mission Area Analyses which identify requirements necessary to effectively accomplish IW/C2W.

(f) The Marine Corps Systems Command conducts research, development, and acquisition activities needed to satisfy IW/C2W requirements.

(g) The Marines are working towards assigning personnel to each of the Service IW centers. They currently have personnel stationed at the NIWA and a liaison officer at the AFIWC, and are trying to place others at the LIWA and the FIWC. Their main focus of effort will be with the FIWC.[27]

4. Comparison of Service Perspectives

a. Terminology

(1) To compare terminology, a distinction must be made between C2W and the realm beyond C2W, be it Information Operations or Information Warfare. In the realm of C2W, the Services are in harmony with the vast majority of terminology used to describe their application concepts. There are isolated cases of divergence. The Air Force uses the term "physical attack" versus "physical destruction" to emphasize the fact that total destruction of an IW target may not be necessary to meet the objectives. The Navy uses the term "counter-C2" to describe the offensive portions

[27] Interview with HQMC PP&O

of C2W, while the other Services and the Joint Staff use the term "C2-attack." The initial drafts of FM 100-6 and Joint Pub 3-13 used the "counter-C2" terminology; however, the latest versions have been changed to reflect the recent transition to "C2-attack." With the exception of the Air Force and their inclusion of Information Attack, the Services are in alignment as to the elements of C2W, and use almost identical discussions to describe the synchronization and orchestration of the five elements to maximize success on the battlefield.

(2) The largest inconsistencies in terminology occurs when the Services describe those operations beyond the limited sphere of C2W. The most obvious example concerns what these operations themselves are called. The Army prefers the term "Information Operations" over "Information Warfare" because they see the need to emphasize the fact that information pervades the entire spectrum of conflict, and that Information Operations occur on a continuous basis, including times of peace [reference para. 3.a.(1)]. Within the Army's Information Operations discussions, they often use the terms IW and C2W synonymously. AR 525-20 (draft) states "The terms C2W and IW are used synonymously because the Army may be called upon to assist with IW and C2W operations, outside of ongoing Army operations, with another Service, joint command, national agency, or allied force. It is possible for the Army to be specifically assigned an IW mission by the NCA through the National Military Command Authority (NMCA) and later assigned a C2W mission by the NMCA or unified/specified command."[28] However, the majority of the application discussion, regardless of whether it is referred to as IW or C2W, can be distilled to command and control warfare as it is defined in MOP 30.

(3) The Air Force and Navy are comfortable using the term Information Warfare, and recognize a distinction between IW and C2W roles for the military. The Air Force has chosen to incorporate IW into existing doctrinal terminology, and therefore uses the term Counter Information, which can be further broken down into Offensive

[28] Army Regulation 525-20, Information Warfare/Command and Control Warfare Policy (draft), page 10

Counter Information and Defensive Counter Information, to describe those missions conducted to control the information environment. The Navy simply refers to Offensive and Defensive Information Warfare.

b. Levels of Conflict:

(1) All of the Services recognize the fact that IW and C2W can be applied across the spectrum of conflict. This is largely due to the power of the media in the new information age. In today's world, traditionally tactical engagements may have overall strategic implications. A prime example is the impact the broadcast of the Task Force Ranger soldiers being drug through the streets of Mogadishu had on the American leadership. However, as the Services discuss the application of IW, there are some apparent divisions in thought.

(2) In looking at the Army's IO concept, one must separate the elements to discuss their application at different levels of conflict. The Army places heavy emphasis on the fact that IO occurs within the Global Information Environment (GIE). They realize the strategic implications that the attainment of informational superiority brings. However, in the offensive realm, the Army focuses on those actions taken at the Corps level and below.[29]

(3) TRADOC PAM 525-69 addresses the following applications at the different levels of conflict:

- Strategic application of IO: The initial focus of IO at the strategic level is on achieving national, alliance, or coalition objectives through intelligence collection and analysis and interaction with the GIE and selected C2W activities such as PSYOP, deception, and OPSEC. As military operations escalate, IO can be employed to disrupt the adversary's information systems, further demonstrating national resolve and military capability.

[29] Interview with DAMO/FDN

- Operational application: The commander formulates the plans for IO as an integral part of the Army's portion of the traditional ground, air, sea, and space operations. The objective is to distort and control the adversary's perception of his battlespace by controlling or corrupting the information he uses, while providing the friendly commander with an unambiguous picture of his battlespace. This includes C2-protect considerations. At this level, commanders must consider how to deal with elements of the GIE, particularly the media and international organizations.

- Tactical application: The commander accomplishes the mission through combined arms operations. He uses IO to disrupt or destroy enemy information systems, primarily through Electronic Warfare and physical destruction. The commander maintains access to his information systems through OPSEC/INFOSEC and electronic protection.[30]

(4) The Marines tend to focus on the operational and tactical applications of C2W. This is in synch with their standing operational doctrine. The Marines view their role in joint warfare to be at the operational and/or tactical versus strategic level of the campaign. Therefore, they are integrating C2W into their doctrine with the same focus.

(5) The Air Force and the Navy tend to lean more towards the strategic applications of IW. The Air Force has extolled the virtues of strategic air power since its inception. By merging information superiority into their basic doctrine, they emphasize the point that information can have the same impact as strategic air power. The Navy sees their forward presence as a key opportunity for the military to apply IW early in a conflict, with the resultant possibility that armed conflict may be completely averted.

---

[30] TRADOC Pamphlet 525-69, Concept for Information Operations, 1 August 1995, pp. 8-9

c. IW as a Strategy or a Means of Warfare: Unfortunately, there is no distinct black and white demarcation between IW as a strategy and IW as a weapon within the Services. Review of the research material available from the Services reveals instances where there are opposing opinions within each Service. Therefore, the following discussion attempts to capture the prevalent themes from each of the Services.

(1) In light of the fact that the Army and the Marines are more focused on C2W than the full range of IW, they tend to approach their development concepts from a strategy viewpoint versus a means. In other words, the integration and synchronization of the five C2W elements are meant to shape the battlefield and permit a rapid, decisive victory following the outbreak of hostilities [reference paragraphs 3.a.(7) and 3.d.(4).]

(2) The Army does address the potential future capability of using IW as a means in AR 525-20 (draft). "The advent of IW/C2W technical applications broadens the scope of strategic military operations. Emerging high technology military capabilities may be employed independently as a stand alone IW action supporting national, diplomatic, and security objectives."[31] However, the majority of their discussion centers on using C2W as a supporting strategy, with the primary goals of creating conditions that lead to dominance in the land force battle and maximizing the friendly commander's effectiveness while degrading the adversary's C2 effectiveness.

(3) The Navy and the Air Force address information as a distinct realm, or "physical entity." Therefore, they discuss IW as a means to attain an objective. They see the need to coordinate and deconflict targeting with the traditional conventional means of warfare. With this view, the Joint Force Commander will have the option of using IW as one more alternative in his arsenal of tools to meet his objectives. Within the Air Force, C2W is occasionally referred to as a strategy or objective, but the

[31] AR 525-20 (draft), page 10

preponderance of the Air Force literature focuses on IW as a means to attain the JFC's objective.

(4) The Navy and the Air Force believe IW is substantive enough to serve as a potential deterrent to armed conflict. This is not to imply that these Services see IW as the panacea for future conflicts. Rather, they stress the need to maintain a strong, modern, viable combat capability. However, they both feel that IW has the potential to prevent or significantly reduce the need for armed conflict to resolve hostilities, in appropriate situations.

5. Common Service Challenges.

While the primary focus of this study is to compare and contrast the Services in the IW realm, several issues can not be classified into concurrent or divergent categories. It is more appropriate to address them as common challenges that all of the Services face.

a. Intelligence

(1) In the realm of Information Warfare, the intelligence community faces a number of significant challenges. First and foremost, we must address our own vulnerability to Information Warfare. The United States military is widely recognized as the most technologically advanced force in the world. Numerous articles have been written extolling our success in Desert Storm, which is often referred to as the first conflict waged in the Information Age. Many of the articles, most notably those written by Russian analysts, emphasize the role information superiority played in attaining our objectives with speed and relatively low loss of life. However, we must acknowledge the fact that potential adversaries recognize our reliance on information, and as such, will likely attempt to deny us the opportunity to gain information superiority in future conflicts.

(2) The intelligence community plays a key role in identifying the capabilities of our potential adversaries. The challenge they face is that in the world of IW, it is

extremely difficult to identify these adversaries. Since the demise of the Cold War, we no longer have the luxury of preparing a defense against a known, quantifiable threat. Today's military faces a spectrum of potential adversaries that may include individual "hackers", insider espionage, terrorist groups, foreign intelligence services, religious and/or cultural factions, as well as nation states. Additionally, easy access to relatively low cost technological advances enable adversaries to attain credible IW capabilities with ease. Therefore, maintaining a current database of potential threats and their capabilities poses a formidable challenge to the intelligence field.

(3) In addition to the defensive arena, there are a number of challenges with offensive IW as well. To achieve precision effects with IW, the commander must have exact intelligence support. As the GIE becomes more intertwined, the intelligence community has a formidable task in identifying critical nodes and links within an adversary's information system, as well as determining the potential for and/or impact of collateral damage. A key objective of IW is to get inside of an adversary's decision cycle. To be able to do this, the commander must not only understand the adversary's C2 system, he must also understand the adversary's decision making style and his vulnerability to C2W strategies. This all results in an exponential growth in intelligence requirements for the commander's Intelligence Preparation of the Battlespace (IPB).

b. Field Training Exercises / Classification

(1) Many of the techniques involved with IW are highly classified. Additionally, some of the techniques may be perishable, losing their effectiveness once they are used. This presents a severe challenge to the Services as they try to integrate IW into their field training exercises.

(2) The ramifications of this challenge are two-fold. First, the inability to fully integrate IW into field training exercises prevents operational planning staffs from synchronizing and orchestrating the full capabilities of the total force. Therefore, it is

difficult to gain a complete appreciation of the abilities and/or limitations associated with IW. Secondly, and most importantly, a lack of IW integration in FTXs results in an education problem. A major factor in developing IW doctrine is the paradigm shift required to understand the possibilities IW opens to the commander. As stated in TRADOC PAM 525-69, IO does not just involve systems, tactics, techniques, and procedures. It is a "total mindset." Limiting IW in FTXs may inhibit acceptance of its value by the people who will be required to integrate it with the commander's concept of operations. Several documents address the need to train for C2W/IW. However, the challenge facing the Services is how to accomplish the training without compromising capabilities.

c. Combat Assessment

(1) The heavy use of precision guided munitions (PGMs) in Desert Storm presented a unique challenge for combat assessment (CA). Traditional methods for conducting CA proved to be inadequate for providing the commander with rapid, accurate assessments. This problem may be exponentially more difficult when assessing the results of IW/IO.

(2) One of the primary elements in IW is physical destruction. The requirements associated with conducting CA in this realm have been thoroughly examined. However, with IW/C2W, new challenges arise. For example, a primary goal of C2W is the disruption of the adversary's decision cycle.[32] Quantifying success at this is proving to be difficult. Additionally, CA in a virtual dimension requires new assessment criteria that the Services are trying to identify.

d. Acquisition Cycles

(1) Technology is expanding at an exponential rate. In the commercial market, computer technology is outdated 18 to 24 months after it is introduced.[33] While IW

---

[32] Joint Pub 3-13 (draft), Joint Doctrine for Command and Control Warfare (C2W), May 1995, pg. I-8
[33] AFIWC briefing given at the LIWA/AOC IW Conference, McLean VA, 24 October 1995

is not solely dependent on technology for success, it is significantly affected by it. The military's current protracted acquisition cycle is not capable of responding to the rapid advances in technology. Therefore, the Services have expressed the need to refine their capability to rapidly integrate new technology into military systems.

(2) This problem is exacerbated by the fact that potential adversaries may not be saddled with this acquisition challenge. Commercial off-the-shelf technology capable of providing a credible IW capability is readily available on the open market. The U.S. military must streamline the acquisition cycle in order to maintain any technological advantage we may currently have.

e. Legal Considerations

(1) Currently, there are very few laws and regulations that govern the use of information systems for IW. This presents a significant challenge to DoD as they prepare Rules of Engagement and Status of Forces Agreements. A common question posed is "At what point does Information Warfare constitute warfare?" This point may be moot given the number of times the United States has formerly declared war in the last 50 years. Many contend that the United States has already been involved in some aspect of IW for years. None the less, the legal bounds of IW have yet to be defined.

(2) Several situations in this area bear highlighting. Every month, the number of military sites subscribing to the Internet increases. Many of these sites now offer their own web site. In addition, many military organizations are now using electronic mail as the primary means of correspondence. DoD must respond to the freedom of information laws and privacy acts while protecting the integrity of these information systems. This presents a new challenge for DoD to protect sensitive information from potential adversaries that may use the Internet to gain unauthorized access to information systems.

(3) A recent study completed by the Science Applications International Corporation (SAIC), entitled Information Warfare Legal, Regulatory, Policy, and Organizational

Considerations for Assurance, discusses many of the legal concerns for IW. A primary consideration is the fact that few countries have laws which adequately address computer crimes. Among those countries that do have computer crime statutes, there is no international agreement on what constitutes computer crime, nor are there any treaties which address computer fraud or abuse. Therefore, it is exceedingly difficult to identify and prosecute international computer criminals.[34]

(4) Many commercial systems can be used to acquire or pass information. As an example, Global Positioning Satellite (GPS) receivers are commonly used by non-military users. Several commercial satellite systems are used to pass communications and imagery support across the globe. During times of conflict, legal constraints may make it difficult for DoD to control access to these systems in an attempt to limit information support to our adversaries.

f. Protection of Shared Use Systems.

(1) DoD relies on commercial systems to transfer the vast majority of information required to sustain operations. This reliance on the commercial information infrastructure makes it a potential target for hostile IW activity. While defensive measures may be taken to protect the integrity of the information passed, DoD must prepare for the possibility of the disruption of these systems. The Communications Act of 1934 is the primary regulation that governs the civilian information infrastructure reliability and availability. While it created the FCC and empowers Congress and the President to protect the telecommunication network, it does not cover all of the considerations for conducting defensive IW. [35]

(2) A recent Defense Science Board study highlights this problem area. "The NSA possesses the critical expertise needed to help protect the Public Switched Network and the larger National Information Infrastructure, but is limited by existing authorities, i.e., the Computer Security Act of 1987, to dealing with federal systems

[34]SAIC, 2-29
[35] SAIC, 2-22

handling classified information. The same Act assigns the National Institute of Standards and Technology (NIST) the role of protecting federal-only unclassified but sensitive information. *No one is responsible for protecting the commercial, public and private systems upon which national viability now depends.*"[36] Therefore, defining the OPR for protection of these systems becomes a key issue. Current initiatives are being taken to identify precisely who is responsible for the protection of the commercial information infrastructure against hostile IW actions.

6. Conclusions.

Based on our research, we offer several subjective conclusions. In the area of Command and Control Warfare, the Services are in agreement concerning the *application* of C2W as a strategy to shape the battlefield. The emphasis in C2W discussion is the integration and synchronization of specific elements to achieve a synergistic effect. With the exception of the Air Force, there is a common understanding of those elements. The Air Force has chosen to make information attack a separate element while the remaining Services incorporate IA techniques into EW and/or destruction categories. While the Services stress the integration of C2W elements as a strategy, not every Service plays an equal role in planning and executing these elements. Support in each of the C2W elements generally follows each Service's core competencies. The primary example involves psychological operations. PSYOP planning is generally the responsibility of the Army. However, each of the Services may play a role in executing the PSYOP campaign (i.e., delivery of leaflets, TV/radio broadcasts, etc.). The primary divergence of opinion occurs in discussion of IW capabilities that go beyond the scope of C2W. This divergence may be attributed to the current lack of *specific* guidance for the full range of the military involvement in IW. Initial guidance focused on C2W as the military application of IW on the battlefield. However, the Services were directed to "organize, train, and equip" for Information Warfare with no specific guidance as to what that

[36] Report of the Defense Science Board Summer Task Force on Information Architecture for the Battlefield, October 1994, pg. 36

may entail. Therefore, it appears that the Services are incorporating IW into their traditional concepts of operations.

a. The Army is engaged in a force modernization plan with the ultimate goal, outlined in the Force XXI vision, of complete digitization of the battlefield allowing seamless command and control from Corps Commander to the individual soldier in the foxhole. A major portion of the Army's Information Operations concept centers on attaining and/or maintaining information dominance through complete situational awareness and expanded vision while denying the adversary the same. The Army's application of IW concentrates on setting conditions that allow the friendly commander to operate inside the adversary's decision cycle. This leads to their emphasis on C2W, information systems, and intelligence as the primary elements of Information Operations. The Army's traditional doctrinal focus has been, and continues to be, on Corps and Division operations. While the IO concept acknowledges the Global Information Environment and the impact IW may have at the strategic level of warfare, the Army's application of IO is primarily focused at enhancing the capabilities of Corps and Divisions at the operational/tactical levels of warfare.

b. Since its inception, the Air Force has stressed the strategic viability of air power. Their capability to bypass the majority of the adversary's fielded forces and directly strike the centers of gravity has been a cornerstone of air power doctrine. The Air Force has taken a similar strategic approach to Information Warfare. By folding IW into their existing doctrine, the Air Force stresses that IW is merely a means to accomplish the operational commander's campaign objectives. The Air Force feels that confining the military role in IW to the boundaries of command and control warfare is too restrictive. The focus of the C2W strategy is to achieve command and control dominance, allowing the commander to operate within the adversary's decision cycle. From the Air Force's perspective, command and control dominance results from the attainment of information superiority, and the adversary's C2 structure is *a* target set that contributes to information superiority. However, the Air Force believes that there are other target sets, that contribute to the achievement of information superiority, that are vulnerable to IW

techniques and may be outside those targets traditionally categorized as C2 targets. The strategic application of IW against an adversary's informational centers of gravity could have the effect of neutralizing his will and capacity to wage war, regardless of the adversary commander's C2 capabilities. This is consistent with the Air Force's doctrinal belief in the strategic application of air power.

c. The Navy's foundational doctrine "Forward ... From the Sea" changed their perspective from a "blue water" strategic focus to a "brown water" force capable of shaping the battlespace from the littorals. Because of their forward presence, the Navy believes that they will be the force initially engaged in the early stages of a crisis to set conditions for any future conflict. This change in perspective recognizes the strategic implications of IW as an enabling function to deter conflict or to establish conditions favorable for joint force operations. C2W has long been an integral warfare area in the Navy's Composite Warfare Commander (CWC) concept. Although terminology has changed, the Navy has been executing the elements of C2W for years. In the past, their primary focus has been the protection of the battle group, primarily through destruction, OPSEC, deception, and EW. However, with the shift in focus to "brown water" operation, the Navy is now expanding their perspective to recognize their ability to shape the battlespace inland as well. This recognition of the strategic implications of IW is based on the probability that naval forces, because of their forward presence, will likely be the first to engage the enemy. Therefore, the Navy is striving to obtain the capabilities to use IW to set the conditions for quick, decisive victory. The Navy sees the need to avoid bounding the military application of IW to command and control target sets. Like the Air Force, they feel that IW techniques can be applied to a wide variety of targets that may be beyond the scope of the traditional C2W target set. The Navy's current challenge is to shift their force protection focus from the battle group to leveraging the capabilities of the battle group and use it as a spring board for the strategic application of IW in a crisis area.

d. The Marines traditionally view themselves as a crisis response force capable of stabilizing an emerging situation, allowing the introduction of follow on forces. They

view C2W as a coordinating strategy at the operational and/or tactical level that enhances the effectiveness of combat operations. The Marines do not envision the development of "IW warriors" in a strategic sense. In their opinion, if a situation requires a military response, conventional applications of force will be required to resolve the crisis. However, the Marines do view C2W as an enabling strategy that leverages the ability of friendly forces to decisively defeat an adversary. Emerging technologies, systems, and techniques in the area of IW must be integrated into the existing constructs of C2W and "fine tuned" to contribute the overall C2W effort. For the near term, the Marines are placing their focus on C2W, and assisting the Joint Staff in determining the full range of the military's role in IW. As DoD and joint perspectives on IW become more clearly defined, the Marines will apply their capabilities to best support the joint force within those requirements and their Service's mission. Doctrine development will follow if necessary.

e. The integration of emerging IW precepts into traditional doctrine enables the Services to place a foundation under relatively ill-defined, and somewhat amorphous concepts. Each of the Services has established a doctrinal baseline based on existing Service paradigms and constructs. However, IW development is in its infancy and we must proceed with caution. Development of IW into a mature capability is dependent on our ability to break traditional military paradigms, and "think outside of the box". This change in mindsets may prove to be the biggest near-term obstacle the Services face as they seek to understand the military implications of the "Information Age".

References

1. Air Force Concept Paper, Cornerstones of Information Warfare

2. Air Force Doctrine Document 1 (draft), Air Force Basic Doctrine, 1 August 1995

3. Air Force Doctrine Document 5 (preliminary draft), Information Warfare

4. Air Force Executive Guidance, 1995

5. Army Regulation 525-20 (draft), Information Warfare/Command and Control Warfare (IW/C2W) Policy

6. Chairman of the Joint Chiefs of Staff Memorandum of Policy No. 30, Command and Control Warfare, 17 July 1990, 1st revision 8 March 1993

7. FM 100-6 (draft), Information Operations, 13 November 1995

8. Joint Pub 3-13 (draft), Joint Doctrine for Command and Control Warfare (C2W), May 1995

9. OPNAVINST 3430.26, Implementing Instruction for Information Warfare/Command and Control Warfare (IW/C2W), 18 January 1995

10. OPNAVINST 5450., Missions, Functions, and Tasks of the Fleet Information Warfare Center (FIWC)

11. Report of the Defense Science Board Summer Study Task Force, Information Architecture for the Battlefield, October 1994

12. Rowe, Wayne J. Strategic Research Department of the Center for Naval Warfare Studies, Information Warfare: A Primer for Navy Personnel, June, 1995

13. Science Applications International Corporation (SAIC), Information Warfare - Legal, Regulatory, Policy, and Organizational Considerations for Assurance, 4 July 1995

14. Stuble, Dan. "What is Command and Control Warfare?", Naval War College Review, Summer 1995, Vol XLVIII, No. 3

15. TRADOC Pamphlet 525-69, Concept for Information Operations, 1 August 1995

Glossary

C2 Attack (Air Force): Any action against any element of the enemy's command and control system.

Command and Control: The exercise of authority and direction by a properly designated commander over assigned 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. (JP 1-02)

Command and Control System: The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned. (JP 1-02)

Command and Control Warfare: The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), 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 operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive:

C2-attack: Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system.

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. (CJCS MOP 30)

Counterinformation (Air Force): Actions dedicated to controlling the information realm.

Direct Information Warfare (Air Force): Changing the adversary's information without involving the intervening perceptive and analytical functions.

Electronic Warfare: 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 EW are: electronic attack, electronic protection, and electronic warfare support. (JP 1-02)

Global Information Environment (Army): Individuals, organizations, and systems outside the sphere of military or National Command Authority control that gather, process, or disseminate information to national and international audiences. (FM 100-6 [draft)])

Indirect Information Warfare (Air Force): Changing the adversary's information by creating phenomena that the adversary must then observe and analyze.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form. (DoD Directive S-3600.1 [draft])

Information Attack (Air Force): Directly corrupting information without visibly changing the physical entity within which it resides.

Information Dominance (Army): The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations short of war, while denying those capabilities to the adversary. (FM 100-6 [draft])

Information Function (Air Force): Any activity involving the acquisition, transmission, storage, or transformation of information.

Information Operations (Army): Continuous military operations within the Military Information Environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. Information Operations include interacting with the Global Information Environment and exploiting or denying an adversary's information and decision systems. (FM 100-6 [draft])

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, store, transmit, display, and disseminate information. (DoD Directive S-3600.1 [draft])

Information Superiority: that degree of dominance in the information domain which permits the conduct of operations without effective opposition. (DoD Directive S-3600.1 [draft])

Information Warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems. (DoD Directive S-3600.1 [draft])

Information Warfare (Air Force): 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.

Information Warfare (JP 3-13 [draft]): Actions taken to achieve information superiority in support of national military strategy by affecting adversary information and information systems while leveraging and defending friendly information systems.

Information Warfare (ASD (C3I)): Actions taken to achieve information superiority by affecting adversary information, information-based processes, and information systems, while defending one's own information, information-based processes, and information systems.
Leveraging: The effective use of information, information systems, and technology to increase the means and synergy in accomplishing Information Warfare strategy. (DoD Directive S-3600.1 [draft])

Military Deception: Actions taken to mislead foreign decisionmakers, causing them to derive and accept desired appreciations of military capabilities, intentions, operations, or other activities that evoke foreign actions that contribute to the originator's objectives. (Proposed for inclusion in the next edition of JP 1-02 by JP 3-58)

Military Information Environment (Army): Military environment contained within the Global Information Environment, consisting of information systems and organizations, friendly and adversary, military and non-military, that support, enable, or influence military operations.
(FM 100-6 [draft])

Operations Security (OPSEC): 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 adversary intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries.

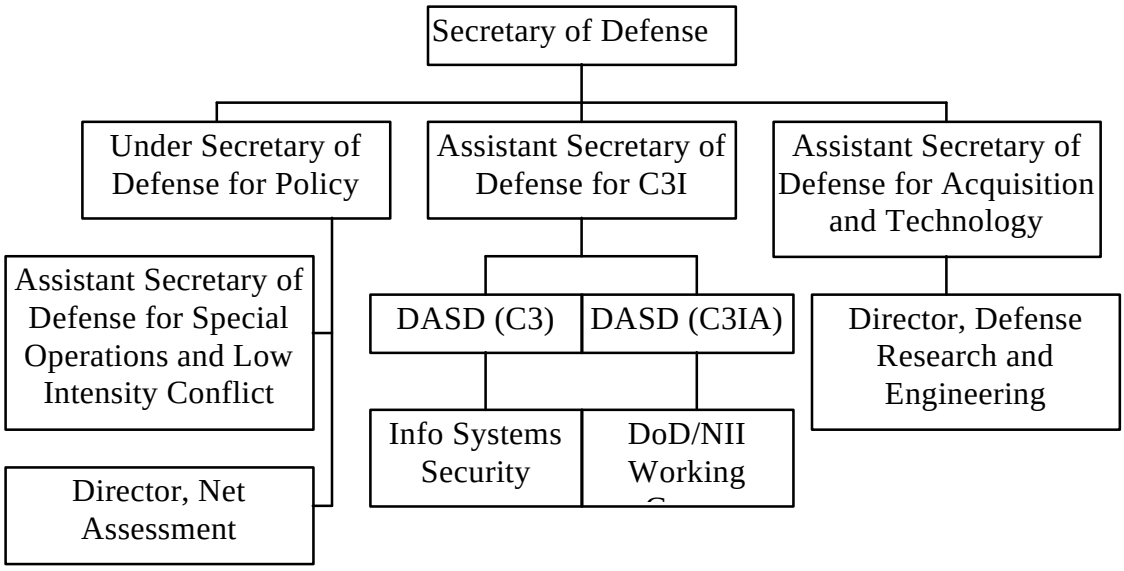
c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. (JP 1-02)

Psychological Operations (PSYOP): 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. (JP 1-02)

APPENDIX A

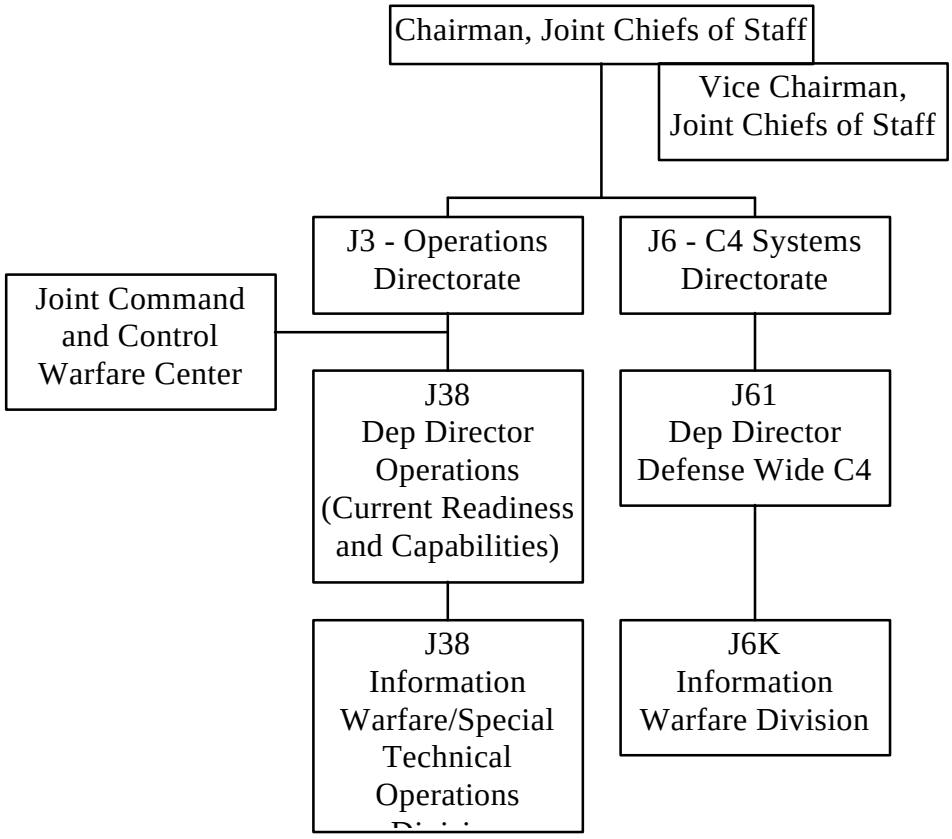
ORGANIZATIONAL DIAGRAMS [37]

Department of Defense

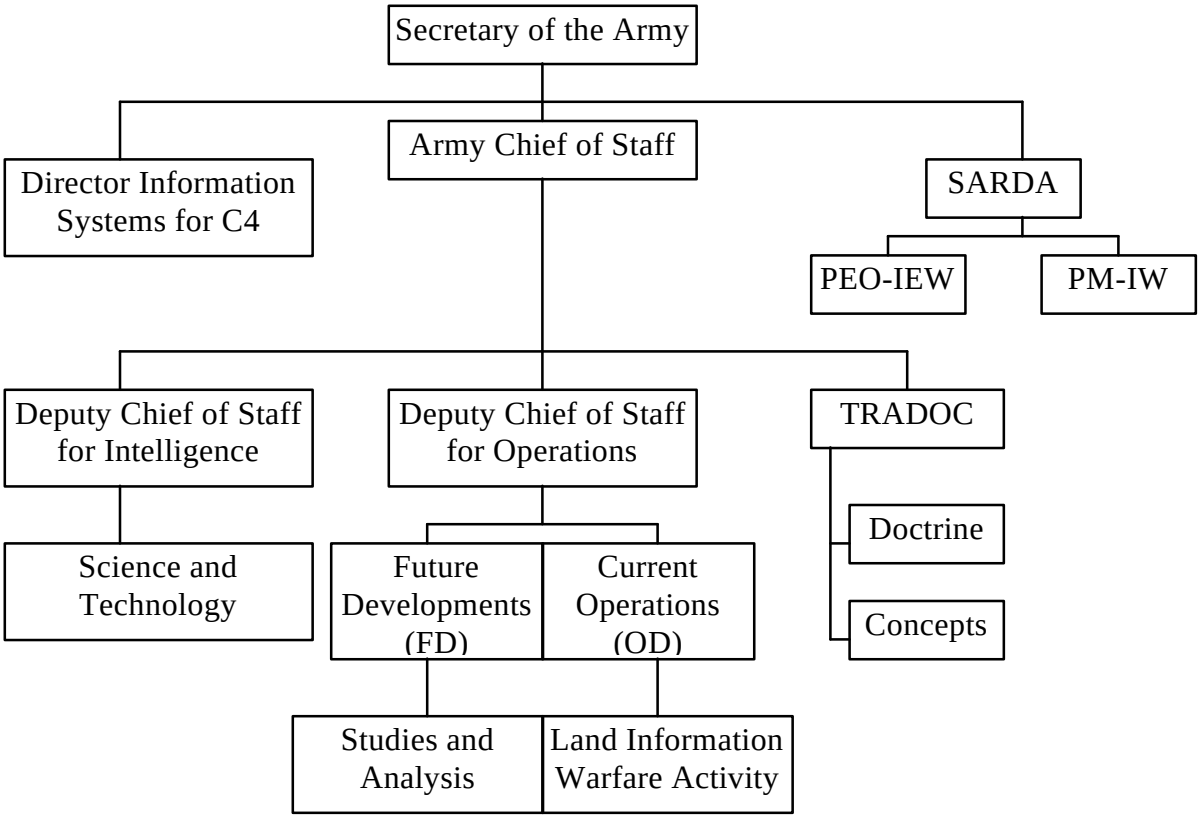


[37] SAIC, Information Warfare, Legal Regulatory, Policy, and Organizational Considerations for Assurance, 4 July 1995

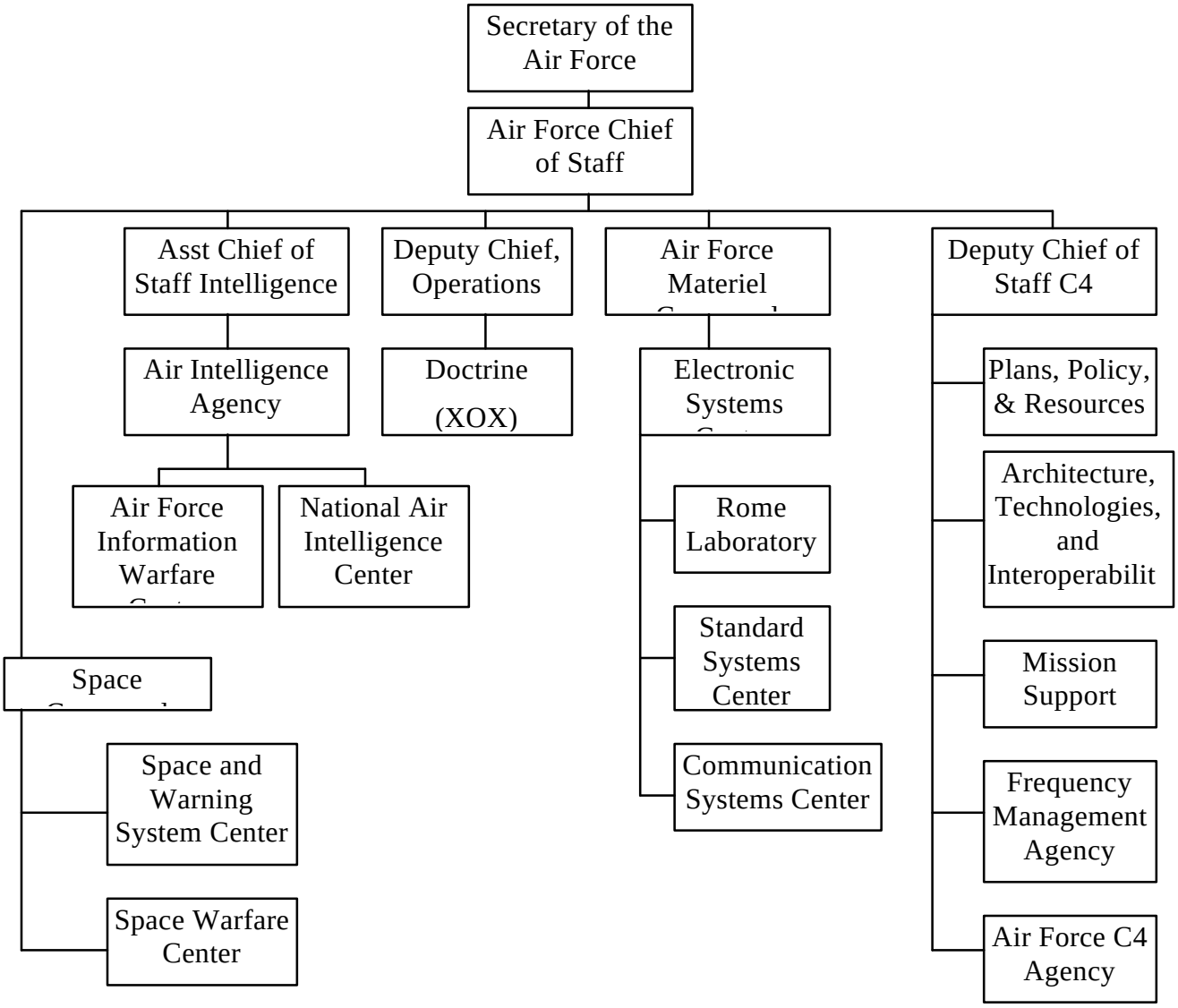
The Joint Staff



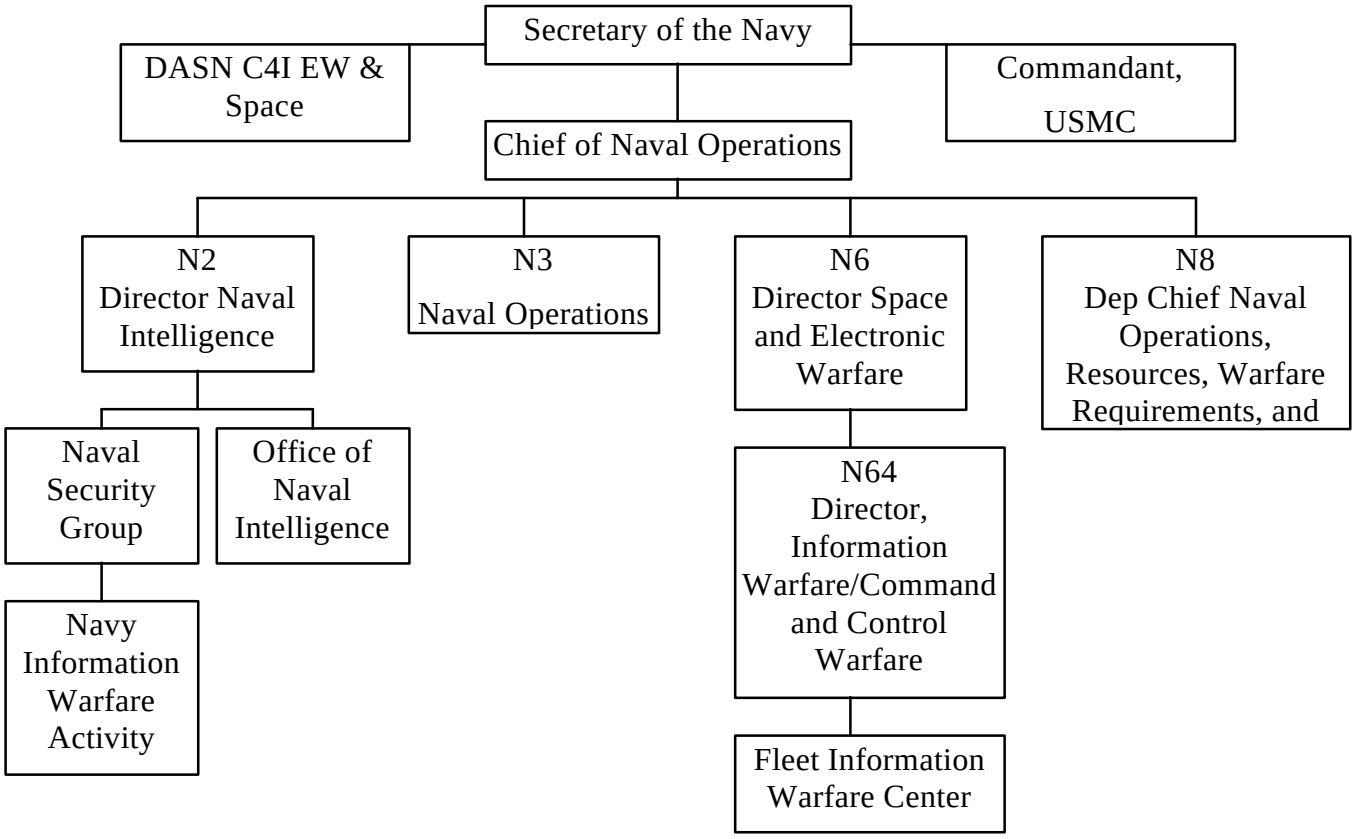
Department of the Army



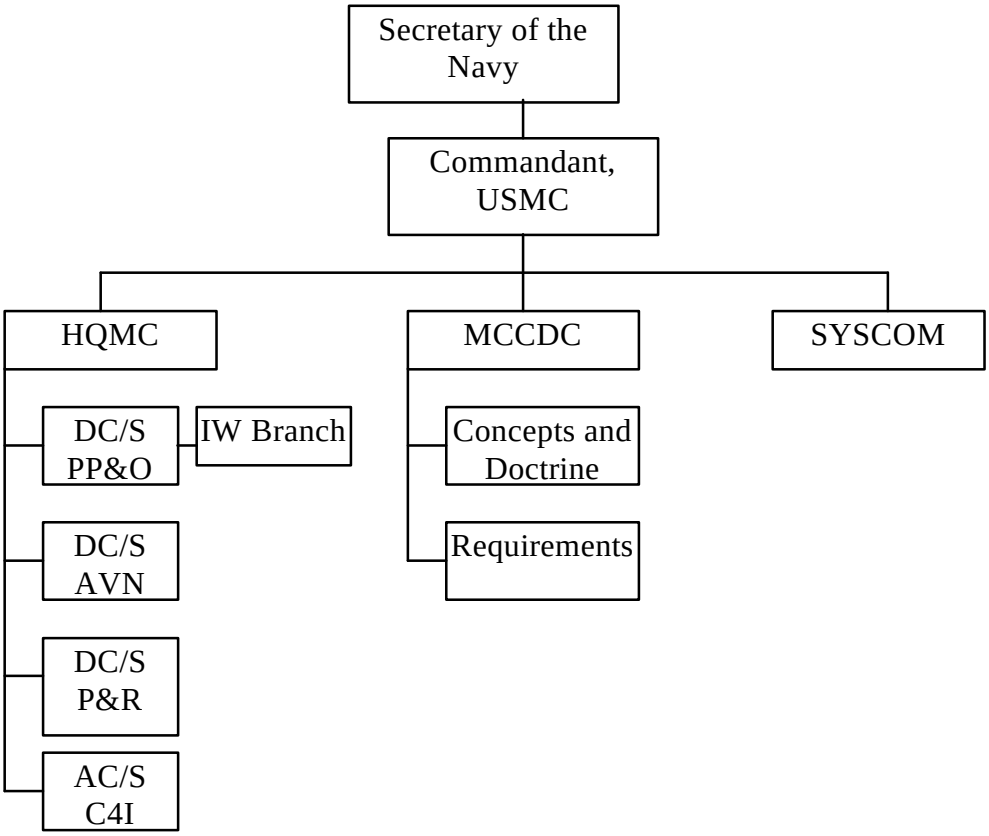
Department of the Air Force



Department of the Navy



U.S. Marine Corps



APPENDIX B

Comparative Analysis of Issues/Synchronization Matrix

Service Doctrine

		Paragraph Reference
Army	***Information Operations*** (C2W + Information Systems + Intelligence)	3.a.(2)
Air Force	***Information Warfare*** as primary focus; C2W as a specific subset	3.b.(3) and 6.b.
Navy	***Information Warfare*** as primary focus; C2W as a specific subset	3.c.(2)
USMC	C2W as a primary focus	3.d.(1) and 3.d.(6)

Primary Elements

		Paragraph Reference
Army	OPSEC, EW, Physical Destruction, PSYOP, and Deception	3.a.(2)
Air Force	OPSEC, EW, ***Physical Attack***, PSYOP, Deception, and ***Information Attack***	3.b.(4)
Navy	OPSEC, EW, Physical Destruction, PSYOP, and Deception	3.c.(3) and 3.c.(4)
USMC	OPSEC, EW, Physical Destruction, PSYOP, and Deception	3.d.(2)

Strategy versus Means of Warfare

		Paragraph Reference
Army	Integrating ***Strategy***	3.a.(7) and 4.c.(2)
Air Force	***Means*** of Attaining Objectives	3.b.(3)(c) and 4.c.(3)
Navy	***Means*** of Attaining Objectives	4.c.(3)
USMC	Integrating ***Strategy***	3.d.(4)

Levels of Conflict

		Paragraph Reference
Army	***Operational*** and/or Tactical	4.b.(2) and 4.b.(3)
Air Force	***Strategic*** and Operational	3.b.(1) and 4.b.(5)
Navy	***Strategic***, Operational, and Tactical	3.c.(4) and 4.b.(5)
USMC	***Operational*** and/or Tactical	3.d.(1)

Coordinating Activity

		Paragraph Reference
DOD	Joint Command and Control Warfare Center (JC2WC)	2.c.(7)
Army	Land Information Warfare Activity (LIWA)	3.a.(8)(c)
Air Force	Air Force Information Warfare Center (AFIWC)	3.b.(9)(e)
Navy	Fleet Information Warfare Center (FIWC)	3.c.(6)(h)
USMC	None as of yet, however, working towards liaisons with other Service Centers	3.d.(8)(g)

Common Issues

	Paragraph Reference
Intelligence	Paragraph 5.a.
Field Training Exercises and Classification	Paragraph 5.b.
Combat Assessment	Paragraph 5.c.
Acquisition Cycles	Paragraph 5.d.
Legal Considerations	Paragraph 5.e.

APPENDIX C

Points of Contact

AGENCY	DSN
Air Combat Command/IN	574-5303
Air Force Doctrine Center	574-8087
Air Force Information Warfare Center (AFIWC)	969-2569
Air Intelligence Agency (AIA)/XRXI	969-2311
Air Staff	
XOXD	225-9066
XOXT	426-5801
Department of the Army	
DAMO-FDN	761-6452
HQ DA DCSOPS/C2W	227-1119
Fleet Information Warfare Center (FIWC)	464-8840
Headquarters Marine Corps (PP&O)	224-3707
J-38	225-3330
J-6	224-5990
Joint Command and Control Warfare Center (JC2WC)	969-4697
Land Information Warfare Activity (LIWA)	235-1791
Marine Corps Combat Development Center, C421	278-6220
National Defense University - Dr. Dan Kuehl	667-9330 ext 366
Naval Doctrine Command	564-0565
Office of the Chief of Naval Operations/N-64	225-0951
OSD(C3I)	224-0622
Training and Doctrine Command (TRADOC)	
DCSDOC/ATDO-F	680-2805
DCSCD/ATCD-B	680-2192