UNITED STATES MARINE CORPS
MARINE CORPS COMBAT DEVELOPMENT COMMAND
QUANTICO, VIRGINIA 22134-5001

15 May 98

Information Operations

Future Marine forces must remain capable of operating effectively across the full range of operations, against a myriad of potential adversaries. ***A Concept for Information Operations*** focuses on a 21st Century information environment of unprecedented complexity, and seeks to identify the essential information operations activities that we must pursue to enable and enhance our warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. This concept is intended to promote discussion and to serve as the catalyst for the process of research and experimentation through which new required operational capabilities will be established. Future developments in information operations capabilities-- in tandem with improvements in other warfighting areas-- will be leveraged by forward deployed commanders to enable the decisive actions envisioned by ***Operational Maneuver from the Sea.***

J. E. RHODES
Lieutenant General, U.S. Marine Corps
Commanding General

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burder for this collection of information is estibated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burder to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (FROM - TO)
15-05-1998		xx-xx-1998 to xx-xx-1998

4. TITLE AND SUBTITLE
Information Operations
Unclassified

5a. CONTRACT NUMBER
5b. GRANT NUMBER
5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Rhodes, J. E. ;

5d. PROJECT NUMBER
5e. TASK NUMBER
5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME AND ADDRESS
United States Marine Corps
Marine Corps Combat Development Command
Quantico, VA22134-5001

10. SPONSOR/MONITOR'S ACRONYM(S)
11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
APUBLIC RELEASE
,

13. SUPPLEMENTARY NOTES

14. ABSTRACT
The Marine Corps warfighting philosophy of maneuver warfare seeks to shatter the enemy?s cohesion through a series of rapid, violent and unexpected actions which create a turbulent and deteriorating situation with which he cannot cope. Marine Corps information operations (IO) support maneuver warfare through actions to deny, degrade, disrupt, or destroy the enemy commander?s ability to command and control his forces. In the future, IO conducted by Marine Air Ground Task Forces (MAGTFs) will consist of battlespace shaping, force enhancement, and force protection activities. Information operations will not be conducted in a vacuum; rather they will complement the traditional uses of military force. MAGTFs will execute IO to enable and enhance their ability to conduct military operations as described in the capstone concept, Operational Maneuver from the Sea (OMFTS).

15. SUBJECT TERMS
IATAC COLLECTION; information operations; information systems; attack

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	Public Release	14	Fenster, Lynn lfenster@dtic.mil
Unclassified	Unclassified	Unclassified			19b. TELEPHONE NUMBER International Area Code Area Code Telephone Number 703767-9007 DSN 427-9007

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	5/15/1998	Report 5/15/1998

4. TITLE AND SUBTITLE
Information Operations

5. FUNDING NUMBERS

6. AUTHOR(S)
Rhodes, J.E.

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

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

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

United States Marine Corps
Marine Corps Combat Development Command,
Quantico, VA 22134-5001

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; Distribution unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The Marine Corps warfighting philosophy of maneuver warfare seeks to shatter the enemy's cohesion through a series of rapid, violent and unexpected actions which create a turbulent and deteriorating situation with which he cannot cope. Marine Corps information operations (IO) support maneuver warfare through actions to deny, degrade, disrupt, or destroy the enemy commander's ability to command and control his forces. In the future, IO conducted by Marine Air Ground Task Forces (MAGTFs) will consist of battlespace shaping, force enhancement, and force protection activities. Information operations will not be conducted in a vacuum; rather they will complement the traditional uses of military force. MAGTFs will execute IO to enable and enhance their ability to conduct military operations as described in the capstone concept, Operational Maneuver from the Sea (OMFTS).

14. SUBJECT TERMS
IATAC Collection, information operations, information systems, attack

15. NUMBER OF PAGES
13

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

A CONCEPT FOR INFORMATION OPERATIONS

Introduction

The Marine Corps warfighting philosophy of maneuver warfare seeks to shatter the enemy's cohesion through a series of rapid, violent and unexpected actions which create a turbulent and deteriorating situation with which he cannot cope. Marine Corps information operations (IO) support maneuver warfare through actions to deny, degrade, disrupt, or destroy the enemy commander's ability to command and control his forces. In the future, IO conducted by Marine Air Ground Task Forces (MAGTFs) will consist of battlespace shaping, force enhancement, and force protection activities. Information operations will not be conducted in a vacuum; rather they will complement the traditional uses of military force. MAGTFs will execute IO to enable and enhance their ability to conduct military operations as described in the capstone concept, *Operational Maneuver from the Sea* (OMFTS).

Information operations at all levels must be carefully planned and fully integrated. MAGTFs must be organized, trained, and equipped to conduct IO in support of a national or theater campaign and in direct support of combat operations. In this context, *Information Operations* is an integrating concept that facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection, not simply another "arrow" in the MAGTF commander's quiver. It is, rather, a broad-based capability that "makes the bow stronger." Thus, the focus of Marine Corps IO will be upon the information-oriented activities that will best support the traditional application of combat power.

Background

The world is in the midst of an information technology explosion--what many are calling an *information revolution*--profoundly affecting all aspects of our lives, including the conduct of U.S. military operations. Military activities on land, sea, and in the air and space affect are affected by information operations. Information has always been important, even decisive, in military operations. The force that best controls, manipulates, and safeguards information and information systems will enjoy a decided military advantage; this will not change. What is new is the speed and volume of information available to military commanders on a near real-time basis, threatening to overwhelm their ability to process data and act in a timely manner.

Information operations exploit opportunities--and minimize vulnerabilities--inherent to dependence on the information that supports military activities. They include actions taken in the information environment by Marine forces to achieve specific results against potential adversaries and are conducted across the full range of military operations. Information Operations target decision makers, information-dependent systems (including weapons), infrastructure, command and control, computers, and associated network systems will play a critical role in supporting the military operations envisioned in Marine Corps warfighting concepts.

The information revolution presents both dangers and opportunities. Dependence on high volumes of timely, accurate information implies risk. It is a vulnerability exacerbated by the likelihood that MAGTFs will operate in austere environments with limited host nation support, at the end of a tether possibly originating in the continental United States. This will present a tempting target for asymmetrical attack by hostile elements unable or unwilling to challenge us directly. All aspects of MAGTF operations, from logistics to intelligence to fire support coordination, rely on increasingly complex information systems that must be protected.

Similarly, opportunity lies in a potential adversary's dependence on information and information systems. As future crises develop, national and theater-level decision makers will more frequently examine potential military responses through the lens of IO. In many situations, U.S. military forces will use IO to exploit critical vulnerabilities that could obviate the need for traditional firepower solutions. The on-scene presence of forward-deployed MAGTFs and their proximity and access to potential crisis areas will establish them as operational and informational "cornerstones" for follow-on forces as part of a national and theater crisis response. Accordingly, the MAGTF must be organized, trained, and equipped to plan and execute IO in support of OMFTS and the joint campaign.

Trends in Technology

Rapid advances in technology have produced an incredibly complex information environment. Routine decisions and interactions have been defaulted to computers in the pursuit of simplicity and speed. Global communications are ubiquitous--e.g. the Internet, satellite/cellular telephones, direct-broadcast television--and expand collective awareness of events, issues, and concerns. Connectivity through global communications will ignite passions, spark perspectives, crystallize beliefs, and compel people, nations, organizations, and institutions everywhere to think and act in accordance with the perspectives, and often biases, of those with whom they interact. While much of this phenomenon may be benign and beneficial, it renders users exploitable.

The United States is at the forefront of exploiting technology to harness the explosive potential of rapid collection, processing, dissemination, and use of information. The U.S. economy, social and civil structures, and governments at all levels have become dependent upon the rapid and accurate flow of information. America exerts extraordinary world influence through its pervasive media and entertainment industries, yet is influenced by similar pressures exerted from outside its borders. The global information infrastructure electronically links organizations and individuals around the world and is characterized by a merging of civilian and military information networks and technologies.

Developments in information technology revolutionize how nations, organizations, and people interact. The rapid diffusion of information challenges the relevance of traditional organizational and managerial principles. The military implications of new organizational sciences that examine networked vice hierarchical management models are yet to be fully understood. Information Age technology and the ideas it fosters greatly influence how military forces organize, equip, train, fight, protect the force, and assist in resolving conflict.

Threats to the information infrastructure come from those motivated by military, political, social, cultural, ethnic, religious, or personal/economic gain. The globalization of networked communications creates new vulnerabilities. The MAGTF's increased linkage to the expanded information infrastructure from points around the world poses a threat from a variety of new and different sources on a continuing basis even during periods of relative peace.

The threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing.

The U.S. military no longer drives the development of information technologies. Commercial off-the-shelf technologies are increasingly important to maintaining the U.S. Armed Forces' technological edge. However, these same technologies are readily available to potential adversaries; adversaries that may be more inventive in adapting these technologies to their operational needs, resulting in apparent chaos and unpredictability. Technology creates missions and functions for Marine forces that are not yet imagined--what might be called "latent demand." Technology is not a panacea and Marines must seek to discover and exploit these new possibilities through a program of aggressive experimentation and operational adaptation.

Information Operations

Information operations involve actions taken to affect adversary information and information systems while defending our own. Aimed to influence decision makers, information operations are applicable across the spectrum of civil-military operations--from peace to crisis to conflict--and at all levels of war.

At the strategic level, IO will be included in the myriad activities directed by the National Command Authority (NCA) to achieve national objectives by influencing or affecting key facets of an adversary's power. As a forward-deployed element of our national power, the MAGTF could be expected to conduct IO at the operational and tactical level to achieve or support strategic objectives. This will require a high degree of coordination between military, government, and non-government agencies.

Information operations consist of offensive IO, defensive IO, and related activities; e.g., civil affairs and public affairs [see Figure 1], and focus the totality of national power on achieving specific national objectives. With the exception of Operations Security and Electronic Protection, all elements of IO are functionally unique; yet considered as a whole, none of them are new. What is new is the complete integration of IO into the Marine Corps' traditional combined arms approach to warfighting.

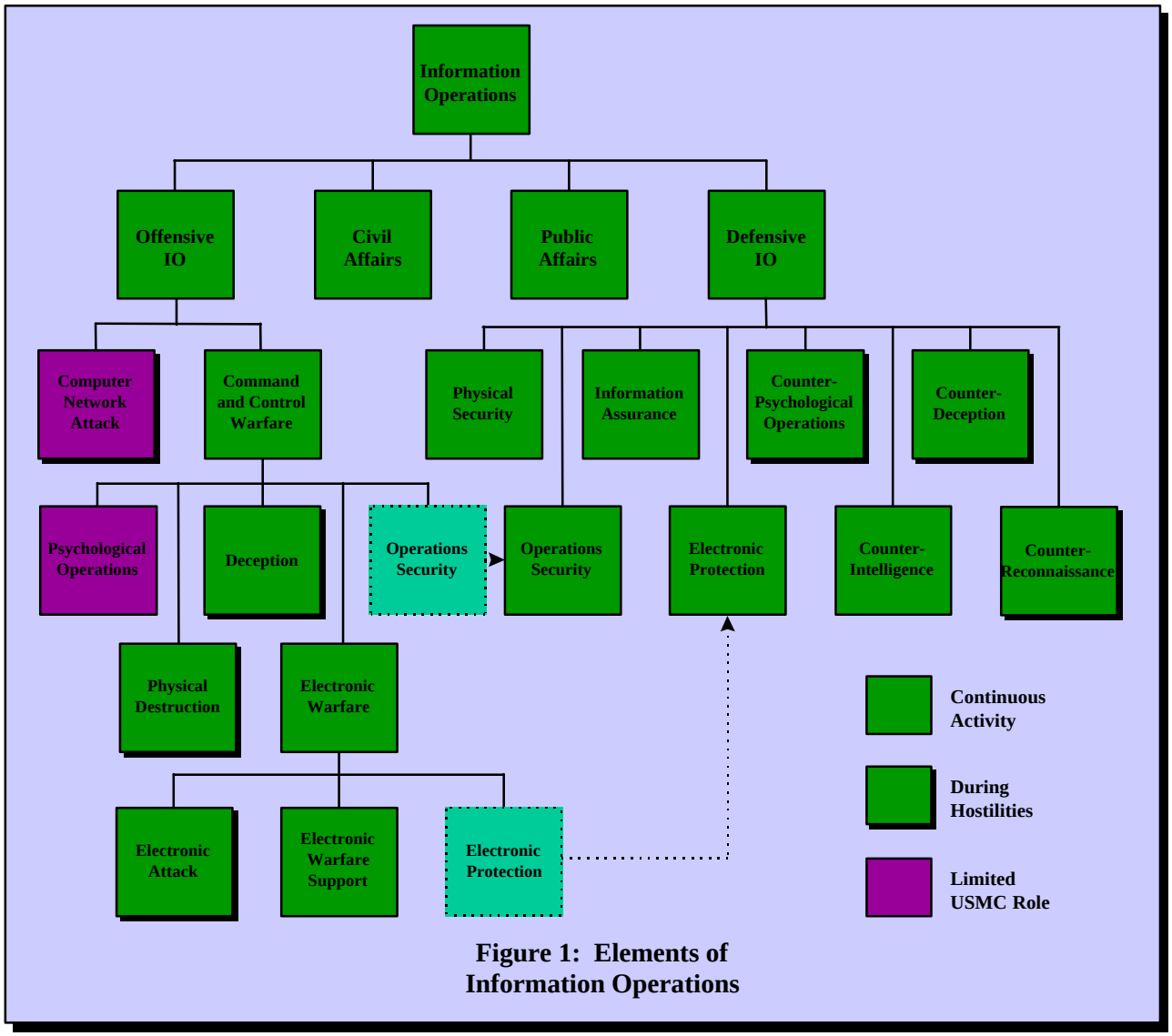

Figure 1: Elements of Information Operations

Offensive IO involve the integration of varied capabilities and activities into a coherent, seamless plan to achieve specific objectives. This guidance must be clearly established, support overall national and military objectives, and include identifiable measures of effectiveness. Offensive IO include the same capabilities that traditionally support command and control warfare, as well as computer network attack and special information operations (those of a sensitive nature posing national security implications, and requiring special review and approval). Human decision making processes are the ultimate target of offensive IO.

Defensive IO integrate and coordinate policies and procedures, operations, personnel, and technology to protect information and defend information systems. Offensive IO can support defensive IO by neutralizing adversary IO capabilities. Defensive IO encompass four interrelated processes:

- *Information Environment Protection*. The MAGTF commander uses policies, procedures, and technologies to ensure freedom of action in the information environment.

Risk management principles must be applied to ensure the most important systems are protected when they are most needed.

- *Attack Detection*. The MAGTF must be able to rapidly detect adversary attempts to attack its information systems, and must be able to differentiate between the effects of adversary action and other phenomena such as weather effects, normal system outages, and operator error. This is essential to ensure effective capability restoration and attack response.
- *Capability Restoration*. The MAGTF requires redundant, resilient information systems that can withstand the effects of enemy action as well as environmental phenomena.
- *Attack Response*. The MAGTF commander can respond to attacks on his information systems by active and/or passive measures. Active measures seek to degrade or destroy the adversary's attack capabilities while passive measures attempt to mitigate the effects of adversary actions.

These activities are conducted in parallel to ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems. Defensive IO are an inherent part of force protection.

Public affairs seek a timely flow of information to both external (public) and internal (government/military) audiences. Coordination of public affairs and IO plans is required to ensure that public affairs initiatives support the commander's overall objectives. The news media and other information networks' increasing availability to society's leadership, population, and infrastructure can have a significant impact on national will, political direction, and national security objectives and policy. Public affairs is a perception management tool that should not be used as a deception capability or to disseminate disinformation to internal or external audiences. In many cases, the ability of public affairs to inject a well-timed truth into the equation can have as significant an impact upon an adversary as a detailed deception plan.

Civil affairs activities are important to IO because of their ability to interface with key organizations and individuals in the information environment, to include non-government and private volunteer organizations (NGOs and PVOs) and their representatives. Civil affairs can support and assist IO objectives by coordinating with, influencing, developing, or controlling indigenous infrastructures in foreign operational areas. Civil affairs and psychological operations involve communicating information and providing support to critical audiences to influence their understanding and perception. Close coordination between public affairs, civil affairs and psychological operations is required to ensure unity of purpose. This is particularly important in the emerging global information environment, as it will often be impossible to restrict dissemination of each message to the intended audience.

Peacetime IO can be used to influence our adversaries through civil affairs and psychological operations to help shape the strategic environment [see Figure 2]. Additionally, public affairs can be used to impart a clearer understanding and perception of our mission and intent. In the pre-crisis stage, preemptive or retaliatory offensive IO can help deter adversaries from initiating actions detrimental to the interests of the United States or its allies. Carefully conceived, coordinated and executed, IO can make an important contribution to defusing crises, reducing the period of confrontation and enhancing diplomatic, economic, military, and social activities,

thereby forestalling and possibly eliminating the need to employ physical force. In the crisis stage, IO can be a critical force multiplier. During combat operations, IO will help shape the battlespace and prepare the way for future actions to accomplish the operational commander's objectives. IO conducted by MAGTFs will consist primarily of force enhancement, force protection and battlespace shaping activities that better facilitate the traditional application of combat power. Once the crisis is contained, IO-- using public affairs, civil affairs, and psychological operations-- will help to restore peace on terms favorable to U.S. national interests.

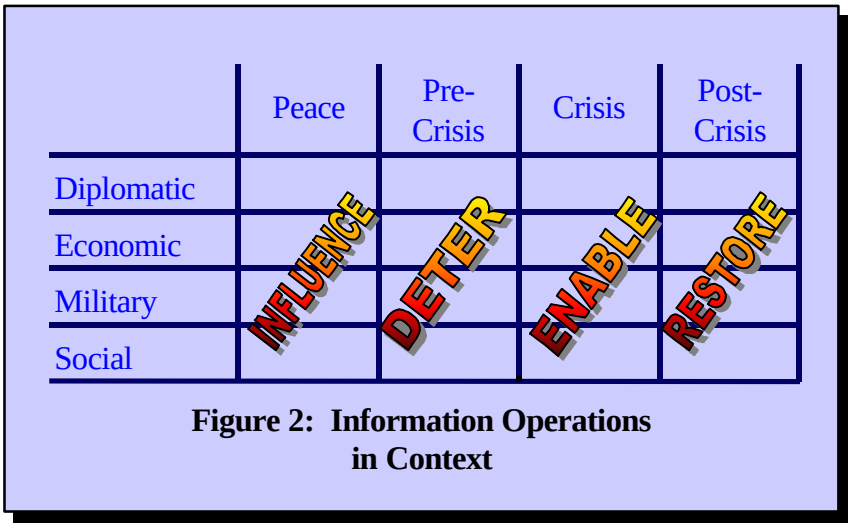

Figure 2: Information Operations in Context

The Marine Corps Role

The global information environment is seamless, requiring information operations to be carefully planned and thoroughly integrated at all levels. Information operations planning must be continuous and incorporated into the normal Marine Corps planning process (deliberate and crisis action). The MAGTF will require robust, resilient connectivity with naval, joint, and coalition forces to plan, deconflict, coordinate, and measure the effects of IO. Since Marine forces will likely fight as a part of a joint force, the MAGTF will rely on national-level agencies and other Service components for certain IO capabilities. Additionally, the MAGTF will require the capability to "reach back" to the U. S. and "reach forward" to personnel or organizations already located in-theater to provide the commander with the ability to significantly increase his situational awareness.

Offensive IO. MAGTFs will conduct offensive IO primarily at the operational and tactical levels to deny or disrupt the adversary's use of information and information systems. The MAGTF commander may utilize electronic attack, physical destruction, psychological operations, and/or deception to prosecute targets related to command and control, intelligence, and other critical information-based processes directly related to conducting military operations [see Figure 3]. A principal focus of offensive IO at this level is the enemy commander and his decision making process. By targeting the human element, we seek to affect the adversary's will to resist. The MAGTF commander's intent is paramount; all elements of MAGTF IO must work together to produce a synergistic effect. The following offensive IO activities conducted by and in support of the MAGTF must be considered:

- Deception is an important enabler for OMFTS and targets enemy decision-makers through intelligence collection, analysis, and dissemination systems. The purposes are to cause adversary commanders to form inaccurate impressions about MAGTF capabilities and intentions, to misappropriate their intelligence collection assets, and to fail to employ combat or support units to their best advantage. Therefore, deception can make a significant contribution to force protection by directing an enemy's combat power away from the MAGTF commander's main effort. There is a price, however, since forces and resources must be committed to the deception effort to make it credible. To ensure consistency, deception operations in support of OMFTS must be carefully coordinated with naval, joint, and coalition deception activities.

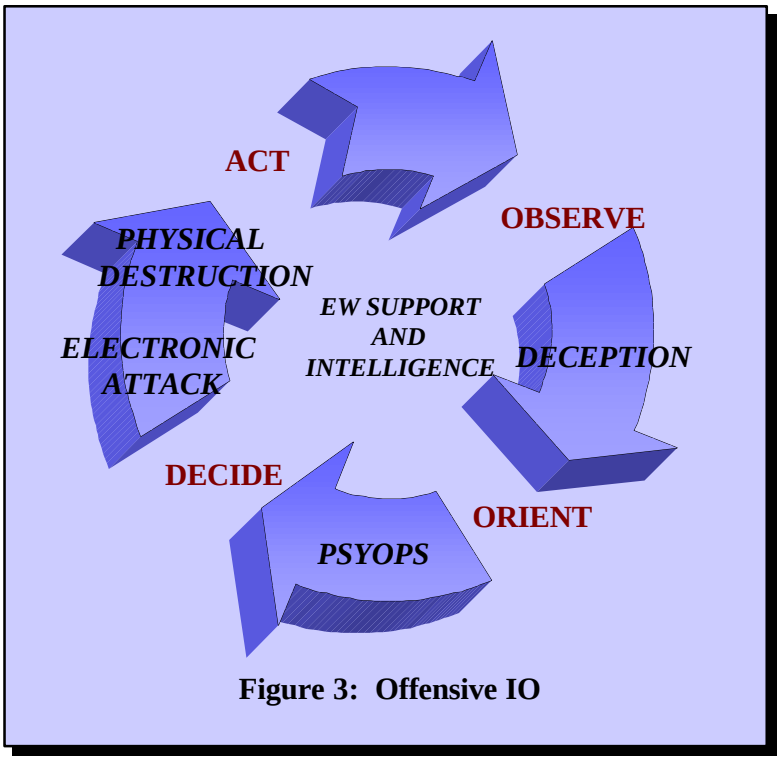

Figure 3: Offensive IO

- Computer network attack is a capability that will be available to the MAGTF commander via other Service components, through resident reach-back capability to national-level organizations, or possibly as an attached special capability. The MAGTF commander must be aware of these computer network attack capabilities and plan for their employment in support of his actions to secure operational objectives.

Defensive IO. The MAGTF commander will depend on information to plan operations and employ his forces. Information systems enable and enhance warfighting capabilities; however, increasing dependence on the rapidly evolving technologies necessary to execute OMFTS creates new vulnerabilities for the MAGTF. Seabasing of the MAGTF command element simultaneously makes information assurance more robust and more difficult to provide. Risk management decisions will have to be made based on the anticipated requirements and information resources most needing protection. Defensive information operations integrate protection, detection, and reaction capabilities to mitigate the effects of enemy action and environmental effects. It also enables the necessary protection of information and information systems upon which the MAGTF depends to conduct operations and achieve its objectives. The criticality of the MAGTF commander's access to, and manipulation of, the information environment will not go unnoticed by future adversaries. [see Figure 4].

Intelligence Support to IO. Offensive information operations require broad-based intelligence support. Intelligence preparation of the battlespace (IPB) in support of offensive IO is a continuous process used to develop a detailed knowledge of the adversary's use of information and information systems. Intelligence support for offensive IO planning builds upon traditional IPB and requires the following:

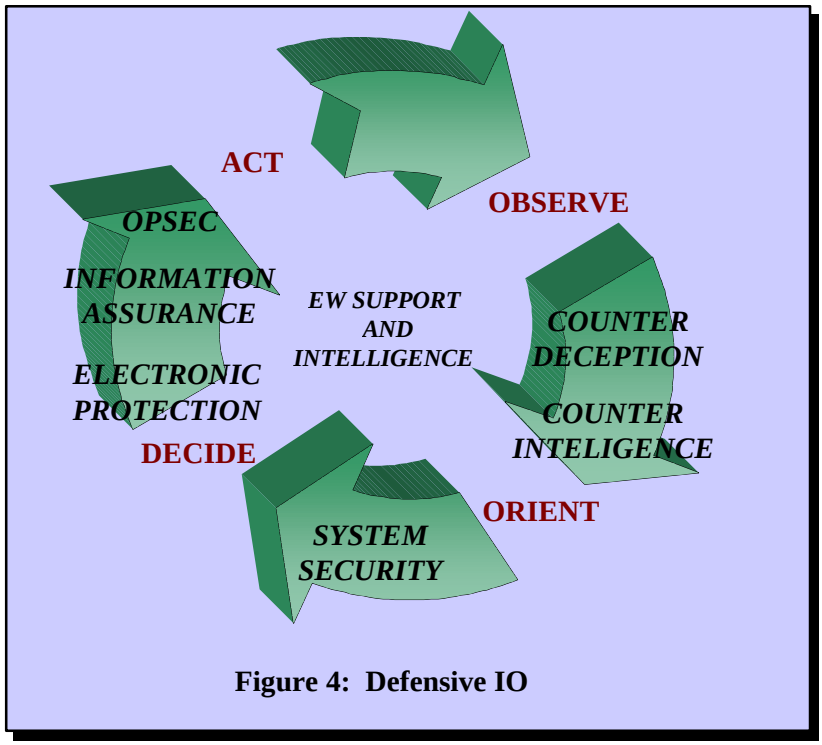

Figure 4: Defensive IO

- v a technical knowledge of a wide array of information systems
- v an understanding of the potential adversary's political, social, and cultural influences
- v an understanding of the adversary's decision making process
- v an in-depth understanding of the biographical background of key adversary leaders and decision makers, to include motivating factors and leadership style

Since IO will often not produce the same directly observable effects utilized for traditional battle damage assessment, IO execution will challenge the intelligence system to develop other measures of effectiveness for these activities.

Intelligence support to defensive IO will require identification of the threat to MAGTF information and information systems. Knowledge of the threat--adversaries, their intent, and capabilities--is a key consideration in the risk management process. Counter-intelligence and counter-reconnaissance contribute directly to force protection by denying critical information to potential adversaries.

Planning for IO. Planning activities are mutually supporting and intended to produce synergistic effects. Offensive IO, for example, can be used to support defensive IO throughout the range of military operations. Offensive IO must be carefully integrated with defensive IO to provide timely response against potential threats to MAGTF information and information systems. Likewise, defensive IO supports offensive IO by mitigating the effects of adversary

Information Operations
In Support Of
Operational Maneuver From The Sea

Operational Maneuver from the Sea describes how a naval expeditionary force will make full use of the options provided by control of the sea. In this example, a naval expeditionary force attacking from Spain has the ability to fight a campaign on the western side of the Atlantic without having to establish a base at some intermediate point. The forces in this example have the option of choosing any one of three Littoral Penetration Areas (LPA).

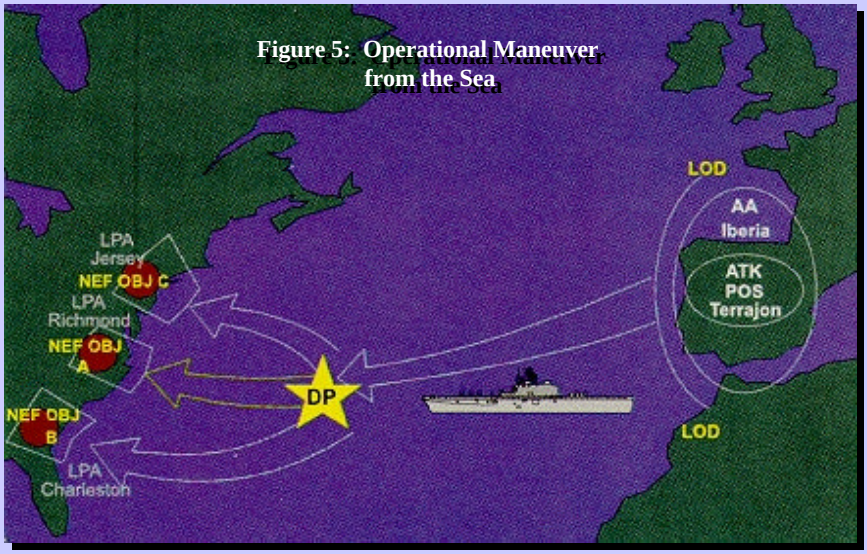

Figure 5: Operational Maneuver from the Sea

Information operations will assist the MAGTF in achieving its specific maneuver objectives. Defensive IO will seek to ensure the availability and reliability of the MAGTF's sea-based C2 systems making sure commanders at all levels have the right information at the right time. Risk management will anticipate requirements and identify resources which need the most protection. This includes both planning for protection and attack response options/capabilities based on the MAGTF commander's information needs, system vulnerabilities, and adversary capabilities. Effective C2 is necessary to ensure that gaps in the enemy's defenses, once identified, can be rapidly exploited. This includes rapid selection of the most vulnerable LPAs and LPPs.

The primary focus of offensive IO will be on affecting adversary decision makers, information systems relating to C2, intelligence, and other information-based processes directly related to the conduct of military operations. Enemy C2 nodes and facilities will be aggressively attacked electronically and with long-range precision fires. Coastal surveillance and integrated air defense systems will be among the first targets. Deception activities will take advantage of the inherent flexibility of OMFTS to present false indicators to the adversary's intelligence system while OPSEC efforts conceal the MAGTF commander's true intentions. PSYOP will undermine the adversary's confidence and will to resist. The MAGTF will thus present rapidly developing situations that preclude effective enemy reaction.

Information Operations…

- is an *integrating* concept
- are an integral part of the MAGTF's combined arms approach to warfare
- focus on an operational objective
- enhance, enable or mitigate the need for traditional combat power
- are conducted continuously
- are an integral part of force protection

actions on the MAGTF commander's ability to effectively employ his forces. Detailed, integrated planning is the key to successful IO. This will require close, continuous interaction and cooperation between all elements of the MAGTF staff, to include some elements which may not be routinely involved in operational planning.

Future Direction

Marine forces must be organized, trained, and equipped to conduct IO in support of a national or theater IO campaign and in direct support of combat operations. In this context, *A Concept for Information Operations* is an integrating concept that enables and enhances the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. This integration can be effectively accomplished by making maximum use of existing force structure and infrastructure. The following considerations will allow Marine forces to take advantage of the opportunities presented by IO on the modern battlefield:

- **Doctrine**. Much of the foundation exists in the form of doctrinal publications, tactics, techniques, and procedures related to the elements of offensive and defensive IO, public affairs, and civil affairs. These functions now must be integrated within the context of the Marine Corps' OMFTS-based warfighting strategy. The Marine Corps planning process must include IO considerations.
- **Organization**. OMFTS is already beginning to drive changes in the way the Marine Corps organizes for combat. Future changes in technology and the information environment will lead to experimentation with new organizational structures which will further validate the emergence of IO as a viable operational concept.
- **Training and Education**. Marines at all levels need to understand the warfighting implications of new information technology and the global information environment envisioned for the future. Awareness will heighten threat appreciation and the importance of adhering to protective measures. Realistic, challenging training will develop the skills required to operate in an austere information environment while mitigating the

IO *In Support Of* OMFTS: Somalia

Operational Maneuver from the Sea contains a vignette which describes how the next generation of power projection forces could carry out simultaneous operations to speed relief to those in need and deprive potentially hostile forces the ability to prepare and react effectively. Information operations will play a central role in ensuring the accomplishment of such missions.

In the pre-crisis phase, national-level policymakers will implement an IO campaign to attempt to defuse the crisis short of military action. At the appropriate time, a naval expeditionary force will be dispatched to the scene to participate in the theater commander's IO campaign. Should efforts to resolve the crisis fail, the force will project power ashore to enable the safe and effective conduct of relief operations.

The naval expeditionary force will conduct continuous defensive IO to ensure the ability to effectively command and control friendly forces and to deny potential adversaries critical information about the force's capabilities and intentions. Public affairs efforts will stress the MAGTF's preparedness to project power ashore should the need arise. Civil affairs personnel will be in close contact with NGOs and PVOs ashore to facilitate planning should forces have to be committed. Planning for potential offensive IO will be closely coordinated with theater and national IO campaign plans.

If committed ashore, the naval expeditionary force will execute high-tempo operations to overwhelm the ability of hostile forces to resist. The naval expeditionary force will use deception, electronic warfare, and, if necessary, lethal force to deny, disrupt, and degrade the adversary's ability to exercise effective command and control of his forces and to resist the MAGTF's actions. Psychological operations will stress the MAGTF's advantages in mobility and firepower and the futility of resistance. Once ashore, the MAGTF will continue to conduct defensive IO to enhance the MAGTF commander's freedom of action.

In many cases, NGOs and PVOs will already be operating ashore when the MAGTF arrives on-scene. In fact, an important MAGTF mission, if not its primary mission, may be to ensure a safe environment for these organizations to do their humanitarian work. Representatives of these organizations will have extensive knowledge about the situation on the ground and could provide access to existing communications or connectivity networks not otherwise available.

vulnerabilities inherent in our information systems and processes. MAGTF exercises should include "Red Teams," that aggressively attack and exploit weaknesses in the MAGTF's information systems. Marine forces must operate effectively even when their information systems fail. Finally, the Marine Corps professional military education system must prepare leaders at all levels for the informational demands of future conflict.

- **Equipment**. OMFTS is also beginning to drive changes in the way the Marine Corps equips for combat. The demands of defensive IO require that MAGTF information

systems be resilient enough to meet the MAGTF commander's requirements while under stress from adversary action and environmental phenomena.

- **Supporting Facilities**. Forward-deployed MAGTFs will increasingly rely on CONUS-based facilities for a wide variety of support functions. The effectiveness of this support will depend on secure, reliable communications, which also must be resilient enough to function while under stress from adversary action and environmental phenomena. The complexity of operations in the information age will tax the ability of the MAGTF staff to effectively handle all of the tasks that will be required. A reach-back capability, also dependent upon secure and reliable connectivity, will be necessary to provide the MAGTF commander with the capabilities he requires to accomplish assigned missions.

Conclusion

The use of information in warfare is not new. Commanders since Sun Tzu have recognized the importance of information in influencing the outcome of battle. The information revolution has evolved from the intersection of knowledge, communications systems, and technology. Information and information technology are no longer simply enhancements to warfare. They are military objectives.

IO Requirements

- Educated Leaders
- Realistic, Challenging Training
- Integrated Planning Process
- Secure, Reliable Information Systems
- Reach-back Support Capability

The information revolution presents both dangers and opportunities. Information operations seek to exploit the opportunities while mitigating the dangers inherent in information systems. These dangers are exacerbated by beliefs that technology will solve problems. Used unwisely, technology can be a part of the problem--contributing to information overload, micro-management and the dangerous illusion that certainty and precision in war are not only desirable, but attainable. Furthermore, all systems that support command and control are potentially vulnerable to enemy action--not just to the physical destruction of facilities and personnel, but also to exploitation and disruption through misinformation, spoofing, hacking, jamming, and other aspects of information warfare. The opportunity lies in "gaps" found in potential adversaries' systems, which the MAGTF will seek to aggressively exploit.

The Marine Corps couples its doctrine of maneuver warfare with technological advances in speed, mobility, fire support, communications, and navigation to rapidly identify and exploit enemy weaknesses. Information operations facilitate the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection. Used wisely, they will serve as a force-multiplier that complements OMFTS and enables the MAGTF commander to operate effectively across the spectrum of conflict.