DEFENSIVE INFORMATION OPERATIONS IN SUPPORT OF THE MARINE AIR GROUND TASK FORCE

A thesis presented to the Faculty of the U.S. Army Command and General Staff College in partial fulfillment of the requirements for the degree

MASTER OF MILITARY ART AND SCIENCE

by

GREGORY T. BREAZILE, MAJ, USMC
B.A., University of Oklahoma, Norman, Oklahoma, 1987

Fort Leavenworth, Kansas
2002

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: Major Gregory T. Breazile

Thesis Title: Defensive Information Operations in Support of the Marine Air Ground Task Force

Approved by:

_____, Thesis Committee Chair
LtCol Richard W. Snyder, M.A.

_____, Member
LtCol Anthony McNeill, B.S.

_____, Member, Consulting Faculty
LTC Debra L. Templeton, M.S.Sc.

Accepted this 31st day of May 2002 by:

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

The opinions and conclusions expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other governmental agency. (References to this study should include the foregoing statement.)

ABSTRACT

DEFENSIVE INFORMATION OPERATIONS IN SUPPORT OF THE MARINE AIR GROUND TASK FORCE, by Maj Gregory T. Breazile, 92 pages.

Currently the Marine Corps has no doctrine for information operations (IO). The Marine Corps Doctrine Division has published an IO concept paper from which to guide the development of IO doctrine. In joint and other service doctrine, IO is defined in both as an offensive and defensive capability. This thesis only discusses defensive IO (DIO) and will attempt to provide the reader with insight into how the MAGTF could conduct DIO. A USMC concept paper on IO, joint IO doctrine, and sister service IO doctrine were used to provide an understanding of how IO and DIO are defined by each. Additionally, analysis of the DIO threat and an overview of current MAGTF capabilities to conduct each of element of DIO (information assurance, physical security, operational security, counterintelligence, counterpropaganda, counterdeception, and electronic warfare) is provided. The thesis also analyzes historical examples of each DIO element to demonstrate relevance of each to MAGTF operations. Conclusions and recommendations are provided for each DIO element. This thesis demonstrates the need for DIO in support of the MAGTF and how the MAGTF should incorporate DIO into their service IO doctrine.

ACKNOWLEDGMENTS

I would like to thank my wife, Marcella and my children, Christopher, Stehpanie, Benjamin, and Cecilia for their support and encouragement during the process of writing this thesis. They provided the inspiration I needed to make this a reality. Without their support, I could have never accomplished this task.

TABLE OF CONTENTS

ABBREVIATIONS

AFCEA	Armed Forces Communications and Electronics Association
AFDD	Air Force Doctrine Document
AM	Amplitude Modulated
CAC	Common Access Card
CERT	Computer Emergency Response Team
CI	Counterintelligence
CIHO	Counterintelligence/Human Intelligence Officer
CINC	Command-in-Chief
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CJTF	Combined Joint Task Force
CNN	Cable News Network
COMSEC	Communication Security
CP	Command Post
C2	Command and Control
C2W	Command and Control Warfare
C4	Command, Control, Communications, and Computers
DCI	Defensive Counterinformation
DIO	Defensive Information Operations
DISA	Defense Information Systems Agency
DOD	Department of Defense

DON	Department of the Navy
DTIC	Defense Technical Information Center
DTRA	Defense Threat Reduction Agency
EA	Electronic Attack
EMW	Expeditionary Manuever Warfare
EP	Electronic Protection
ES	Electronic Warfare Support
EW	Electronic Warfare
FAS	Federation of American Scientists
FCIP	Foreign Counterintelligence Program
FM	Frequency Modulated
FWF	Former Warring Factions
GIE	Global Information Environment
GIG	Global Information Grid
G2/S2	Intelligence Staff Officer
G3/S3	Operations Staff Officer
G6/S6	Communication Staff Officer
HARM	High Speed Antiradiation Missile
HET	Human Explotation Team
HQ AFDC	Headquarters Air Force Doctrine Center
HQDA	Headquarters Department of the Army
HQMC	Headquarters Marine Corps
HUMINT	Human Intelligence

IA	Information Assurance
ICC	Integrated Circuit Chip
IIR	Intelligence Information Report
INFOSEC	Information Security
INFOSYS	Information Systems
IO	Information Operations
ISMO	Information Systems Management Office
IT	Interrogation
IW	Information Warfare
JITC	Joint Interoperability Test Command
JP	Joint Publication
JOPES	Joint Operation Planning and Execution System
JSIVA	Joint Staff Integrated Vulnerability Assessment
JTF	Joint Task Force
LAV	Light Armored Vehicle
MAGTF	Marine Air ground Task Force
MAPI	Messaging Application Programming Interface
MARFOR	Marine Forces
MEF	Marine Expeditionary Force
MCDD	Marine Corps Doctrine Division
MCDP	Marine Corps Doctrinal Publication
MCO	Marine Corps Order
MCPP	Marine Corps Planning Process

MCRP	Marine Corps Reference Publication
MCWP	Marine Corps Warfighting Publication
MIE	Military Information Environment
MOS	Military Occupational Specialty
MSTP	Marine Air Ground Task Force (MAGTF) Staff Training Program
NATO	North Atlantic Treaty Organization
NCIS	Naval Criminal Investigative Service
n.d.	No Date
OCI	Offensive Counterinformation
OMFTS	Operational Manuever from the Sea
OPCON	Operational Control
OPSEC	Operations Security
PC	Personal Computer
PIR	Priority Intelligence Requirement
PKI	Private Key Infrastructure
POG	Psychological Operations Group
PSYOP	Pyschological Operations
TECOM	Training and Education Command
TF	Task Force
TSCM	Technical Surveillance Countermeasures
TV	Television
UHF	Ultra High Frequency
UN	United Nations

UNITAF	United Task Force
UNOSOM	United Nations Operations, Somalia
US	United States
USMC	United States Marine Corps
USS	United States Ship
VHF	Very High Frequency
V/STOL	Vertical and/or Short Take-Off & Landing
WO	Warrant Officer

ILLUSTRATIONS

Figure Page

TABLE

Table Page

CHAPTER 1

INTRODUCTION

Background

Currently, the Marine Corps has no service doctrine for Information Operations (IO). This lack of IO doctrine complicates matters for the Marine Air-Ground Task Force (MAGTF) planners because they have no established process for integrating IO into their operations. The MAGTF is the focus of Marine Corps doctrine because it is how Marine forces are normally organized for combat. The MAGTF is a task organized Marine fighting force consisting of a command element, ground combat element, aviation combat element, and combat service support element under one commander. MAGTFs range in size and capabilities depending on the operational mission. A large MAGTF might be formed around a Marine division while others might be designed for special purposes and formed around small units with unique capabilities tailored to the mission. MAGTFs can be designed to operate in all levels of conflict from high intensity warfare to small-scale contingencies. All MAGTFs are highly trained fighting forces made to integrate the elements of combat power under a single commander, and because of this, must incorporate IO into the combined arms team. The ability to conduct IO and specifically defensive IO (DIO) within the MAGTF will be the focus of this research.

The disestablishment of the Soviet Union changed the world from a bipolar situation, where the Soviets and the US shared superpower status, to a unipolar condition where the US is the only remaining superpower. This superpower status has created a situation where lesser nations vie for positions of influence and attempt to establish solvent economies within the global arena. While the US has gained in status, many

nations that shared power from the Soviet regime have fallen in decline. Many of these are underdeveloped nations that had ties to the Soviet Union and have lost their source of trade and military protection from the once powerful alliance.

This change in world order has created new challenges for the United States. Old hatreds amongst various factions throughout the world have reemerged creating chaos throughout many parts of the globe. The hostile events ongoing in the Balkans are an example of the chaos that resulted from the fall of the Soviet Empire. These changes are difficult for Americans and other Western people to grasp since the changing environment is unpredictable and ill defined.

Due to world changes, these chaotic environments make terrorism a greater threat to US interests. Since the US cannot focus its limited intelligence assets on one or two major threats, the task of tracking terrorist groups throughout the world becomes even more challenging. Anthony H. Cordesman, in his testimony to the Senate Judiciary Subcommittee on technology, terrorism, and government, stated: "At present the US government focuses most of its intelligence analysis, defense planning and response, around a relatively narrow definition of terrorism. It focuses on independent terrorist groups, and not on the threat states can pose in asymmetric warfare. Yet, it is states that have the most access to weapons of mass destruction--particularly biological and nuclear weapons--and which have the most capability to launch sophistication [sic] attacks on our information systems" (Cordesman 2001, 2-3). This challenge of defining the terrorist threat is enormous. The ability to focus collection assets and circumvent a terrorist act may be beyond the abilities of the US intelligence community.

The changing world order has also experienced a rapid technology explosion that has created new potential threats to US military information. The expansive nature of the global information infrastructure invites many hostile parties around the world to target US interests without leaving their own homelands. Military planners must consider the easily exploitable vulnerabilities introduced by the dependence on Internet technologies and the commercial information infrastructure. In James Adams' article *Virtual Defense – The Weakness of a Superpower,* he states:

> The US military stands as an uncontested superpower both conventional and nuclear force. Ironically, its overwhelming military superiority and its leading edge in information technology have also made the United States the country most vulnerable to cyber-attack. Other nations know that they have fallen behind in military muscle, so they have begun to look to other methods for bolstering their war-fighting and defense capacities--namely, "asymmetrical warfare," which the Pentagon characterizes as countering an adversary's strengths by focusing on its weaknesses. (Adams 2001, 98)

Defense of these potential threats is still fairly new and not well understood by US planners. These threats to US information require constant analysis and new tools to defend against them. Defending against these potential threats by focusing on the protection of our military information has made IO a relevant and extremely important topic of discussion in this new century. Ronald R. Fogleman's remarks on IO as the fifth dimension of warfare point out the affect of information on military operations: "Information has an ascending and transcending influence--for our society and our military forces. As such, I think it is appropriate to call information operations the fifth dimension of warfare. Dominating this information spectrum is going to be critical to military success in the future" (Fogleman 1995, 1).

As previously stated, IO must be considered during all phases of military planning. The integration of IO into all US military operations must be done to ensure information superiority remains with US forces. Unfortunately, there are relatively few military personnel that have worked all elements of IO and therefore, no great depth of experience exists on this subject. Many military strategists have written on the subject of IO, but few have actually worked in the IO arena for any length of time. Even US military doctrine on IO is still in its infancy. Army Field Manual 100-6, *Information Operations*, was published in August 1996. This publication laid the foundation for the development of other service and joint doctrine on IO. In August 1998, the Air Force published Air Force Doctrine Document 2-5, *Information Operations*. In October 1998, the Joint Staff published Joint Pub 3-13, *Joint Doctrine for Information Operations*. The Marine Corps has yet to produce any IO doctrine, but may use joint and other service doctrine to assist MAGTF planners in the preparation of IO plans. The lack of doctrine complicates the integration of Marine Forces into the joint IO planning process.

Current joint doctrine addresses IO as both offensive and defensive. This thesis will focus on the MAGTF since this is how Marine forces are task organized under a single command and structured to accomplish a specific mission. This thesis will explore how these task-organized forces can integrate DIO into the planning and execution of MAGTF operations. Joint doctrine defines DIO as:

> the integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. DIO are conducted through information assurance, physical security, operations security, counterdeception, counterpsychological operations, counterintelligence, electronic warfare, and special IO. DIO ensure timely, accurate, and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes. (CJCS 1998, GL-5)

A review of current Marine Corps operational doctrine and concept papers, and an analysis of current joint doctrine may provide an understanding of how the MAGTF might resolve this situation and develop IO doctrine to support it.

The lack of Marine Corps DIO doctrine is dangerous due to the changing nature and proliferation of information technologies throughout the world. Even though the Marine Corps has made great strides in protecting its information systems from computer attacks, it remains that no one doctrinal document ties together all elements of IO under a single umbrella, ensuring actions taken by one element are complimentary to the other elements. The need for elements of DIO to protect information with better encryption and trained network administrators has become necessary to maintain vital information systems. Taking this network centric focus is necessary because of the Marine Corps' dependence on the Internet and commercial information systems to carry essential information. Computer network defense has gained vast publicity due to recent worldwide network virus attacks. Military planners must understand that Information Assurance (IA) is only one piece of DIO. The other elements of DIO (counterintelligence, counterpropaganda, operations security, physical security, counterdeception, and electronic warfare) are also critically important and demand attention.

This thesis will attempt to answer the question of what doctrinal principles are necessary to enable the MAGTF to conduct DIO. Focus on the MAGTF will be based on those elements of DIO described in joint doctrine and the Marine Corps concept paper on IO: "Information Operations is an integrating concept that facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force

protection . . . thus, the focus of Marine Corps Information Operations will be upon the information-oriented activities that will best support the traditional application of combat power" (MCDD 1998, 1). The USMC concept paper focuses on the trends in technology that have changed the operating environment. The ability to rapidly collect, process, disseminate, and use information have altered the way people, organizations, and nations react. The writers of this concept paper focus on the MAGTF and its proximity to potential crisis, making them first in the fight regarding IO. The speed and mobility of a deployed MAGTF qualify them to be a useful tool to the operational level commander, therefore the operational commander must include them in his IO plan. The USMC concept paper describes IO in three major categories: offensive, defensive, and related activities.

As previously stated, my research thesis will focus on the defensive elements of IO as defined in this concept paper. The Marine Corps concept paper defines DIO as:

> Defensive Information Operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect information and defend information systems. Offensive Information Operations can support Defensive Information Operations by neutralizing adversary Information Operations capabilities. Defensive Information Operations encompass four interrelated processes: Information Environment . . . Attack detection . . . Capability restoration . . . Attack Response . . . 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 Information Operations are an inherent part of force protection. (MCDD 1998, 5-6)

This concept paper goes on to describe the Marine Corps' role in IO. It states that IO must be integrated with naval, joint, and coalition forces. It states, "that IO must be integrated with naval, joint, and coalition forces . . . 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" (MCDD 1998, 7). This thesis will research those elements of support required by the MAGTF to execute DIO and what augmentation they will require from other services and agencies.

Purpose

Currently the US Marine Corps is posturing for the future by developing advanced amphibious warfighting capabilities. These advanced capabilities are in line with the vision of Marine Corps concept paper, *Operational Maneuver from the Sea (OMFTS)*. The investment made to purchase such highly evolved equipment such as the MV-22 Osprey (vertical/short takeoff and landing (V/STOL) transport aircraft) and the advanced amphibious assault vehicle, will change the way Marines are employed from the sea. This investment into future capabilities should also seek to provide Marines with the tools to conduct DIO.

Research Question

The primary question this research thesis will seek to answer is: What are the doctrinal principles that will enable the MAGTF to conduct defensive information operations? The historical research methodology will be used to answer this question.

Definition of Doctrine

Field Manual (FM) 101-5-1/Marine Corp reference Publication (MCRP) 5-2A, 1997, *Operational Terms and Graphics*, defines doctrine as the "fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives" (HQDA and HQMC 1997, 1-55). This definition of doctrine will be used during the composition of this thesis.

Subordinate Questions

This thesis will seek to answer several subordinate questions with a focus on how the MAGTF can conduct DIO. The following subordinate questions will be discussed:

1. What is IO? This question will be discussed in detail in chapter 2 of this thesis.
2. What is Defensive IO? This question is answered in chapter 2.
3. How does the Marine Corps define DIO in the Marine Corps Concept Paper on IO? This question will be answered in chapter 2.
4. What is the IO threat to MAGTF Operations and how is the Marine Corps postured to meet that threat? This question will be answered in chapter 3.
5. Using historical lessons learned what standards can be applied to DIO for use by MAGTF Planners? Are these standards relevant at this time or must the MAGTF adapt new standards to meet the current threat? These questions will be answered in chapters 4 and 5.
6. What elements of DIO must the MAGTF perform and what elements can another service or agency satisfy? This question will be answered in chapter 5.

Definitions

Throughout this thesis many military terms will be used. The definitions of each will be defined in the body of this thesis. Chapter 2 will explain the definition of IO and DIO and the elements of each.

Assumptions

The first assumption made at the start of this research was that there are relatively few military planners with IO experience and that IO is still a somewhat new concept that is not well understood throughout the US Military. The second assumption is that

historical examples of IO will be available for research. The third assumption is that the lessons learned from these examples can be applied to MAGTF operations.

Limitations

Due to the global impact made by rapidly changing technologies, the IO threat continues to change. This means that the writings on IO may quickly be outdated by new technologies. Additionally, since IO is not well understood, determining the threat becomes difficult. With the interdependence of information systems throughout the world threats can exist from any part of the globe. Because we do not always understand the threats, we are often put in the position of reacting to an attack rather then preventing one. DIO threats to the MAGTF will be researched in this thesis. Additionally, since there are few individuals throughout the Marine Corps that have worked in the DIO arena researching this topic from the Marine Corps perspective will be difficult. In some cases conclusions will have to be made using sister service examples.

Delimitations

To narrow the focus of this thesis there are several delimitations to this research. The delimitations include:

1. This thesis only discusses MAGTF operations.
2. This thesis only focuses on broad doctrinal principles.
3. This thesis only discusses likely threats to a MAGTF's ability to conduct DIO.
4. Due to the need to include current military technologies, only historical examples that have occurred in recent years will be used during this research.
5. This thesis only covers DIO doctrine that is achievable by deployed MAGTF's.

6. The legal or moral aspects of executing IO will not be considered in this thesis.
7. This thesis will remain unclassified.

Initial Research Design

The historical approach will be the research design used for this thesis. This approach uses the following steps:

Step 1: Define IO and DIO.

Step 2: Conduct a literature of major IO and DIO publications.

Step 3: Identify and analyze the DIO threats.

Step 4: Study MAGTF DIO capabilities.

Step 5: Study historical DIO examples.

Step 6: Make doctrinal recommendations.

Significance of Study

This thesis is relevant to current MAGTF operations since the defense of information and the systems used to manipulate information are so vital to MAGTF commanders and staffs. The defense of vital information will have a significant impact on the future battlefield. Since attackers can position themselves anywhere in the world for such an attack, the military planner must consider defensive measures to protect their vital information.

Literature Review

Currently, the most valuable information pertaining to this thesis is the Marine Corps concept papers on IO and OMFTS. Additionally, Joint Pub 3-13 will provide the joint view of IO and the framework for incorporating Marine forces into the IO process.

Furthermore, a study of recent military operations throughout the spectrum of warfare will be incorporated to ensure a historical perspective on how IO has impacted previous military operations. There are many resources available for the study of DIO. These works will be used in conjunction with recent operational reports to draw some conclusions as to the effectiveness of DIO and how those events can be related to MAGTF Operations. Reading various writings such as Robert Bunker's work titled *Information Operations and the Conduct of Land Warfare*, will provide a foundation from which to draw some conclusions.

Research Design

As previously stated, the research method for this thesis will be based on the historical method. This process will first define IO and DIO. Secondly, it will define the threat. The third step will be to review recent historical examples of how IO was used during military operations. The fourth step will be to study MAGTF DIO capabilities and show areas of DIO that cannot be accomplished by the Marine Corps. The fifth and last step will be to draw some conclusions and make doctrinal recommendations. This method will provide the reader with insight and an understanding of the key operational issues related to DIO and the MAGTF.

CHAPTER 2

LITERATURE REVIEW

This chapter will review current Marine Corps operational concepts along with joint and other service doctrines to enable a proper analysis of how DIO can be integrated into MAGTF operations. Selected writings on the different elements of DIO will be used to better describe to the reader what each of these elements entails. The elements of DIO that will be discussed are counterintelligence, counterdeception, counterpsychological operations, operations security, information assurance, physical security, and electronic warfare. Many articles have been written on these DIO elements, but to keep the focus of this thesis narrow, only selected works will be used in the analysis.

Marine Corps Concept Papers

The recently published Marine Corps concept paper, *Expeditionary Maneuver Warfare (EMW), Marine Corps Capstone Concept* is the single document that will drive all future Marine Corps doctrine. This document outlines the Marine Corps core competencies. It also highlights the fact that Marine Corps forces are expeditionary, ready to deploy anywhere in the world at a moment's notice. This paper goes on to explain how this expeditionary nature gives Marine forces a strategic role since they can be positioned globally to provide a powerful ready combat force. Since Marine forces are ready when others are not, they typically become the force of choice for many types of military operations. This concept paper describes how Marine forces can be used as an enabling force for joint and multinational operations. The capabilities that the deployed MAGTF brings, can provide the core of a joint task force (JTF) and combined joint task force (CJTF). This paper goes on to discuss how maneuver warfare is the philosophical

foundation for EMW. The EMW concept discusses the advantages of sea-basing forces, which enables them to be positioned in different theaters around the globe. Sea-based MAGTFs can also be used to meet strategic objectives. The paper continues on to discuss organization, deployment, and employment as well as maneuver, intelligence, integrated fires, logistics, command and control, force protection and information operations. EMW is an eleven-page document that only briefly touches on these concepts to provide the basis for the development of service doctrine. EMW concludes with the figure 1, which visually depicts what is written in the text of this document. This figure shows how the Marine Corps used the national security strategy, national military strategy, joint vision, and naval vision to develop the Marine Corps vision that is titled *Marine Corps Strategy 21*. This Marine Corps strategy is used to develop Marine Corps warfighting concepts. These concepts will be developed through innovation, Marine Corps heritage, and evolution of combat capabilities. This entire process provides the Marine Corps with the EMW capability that they require.

To provide more clarity on the *Marine Corps Strategy 21,* General James L. Jones, Commandant of the Marine Corps, writes, "Marine Corps Strategy 21 provides the vision, goals, and aims to support the development of future combat capabilities. It provides our strategic guidance to the active and reserve Marines, sailors, and civilian personnel who will make America's Marines, win our Nation's battles, and create quality citizens by optimizing the Corps' operating forces, support and sustainment base, and unique capabilities; and capitalizing on innovation, experimentation, and technology" (HQMC 2000, Forward). These two documents, EMW and Marine Corps Strategy 21, are the cornerstone for all Marine Corps doctrinal developments.

Figure 1. Marine Corps Strategy 21 (HQMC 2001c, 11)

In addition to the EMW and Marine Corps Strategy documents, a review of the Marine Corps concept paper on IO is appropriate. Similar to other service doctrinal publications, this document describes the new operating environment and trends in information technologies. The paper briefly describes the threat to Marine Corps information due to the globalization of communications networks. The paper uses the joint definition of IO and like the joint doctrine, defines IO as both offensive and defensive. Figure 2 is included in the USMC concept paper. This figure depicts the different elements of DIO and how they are used during the operational decision cycle. The paper describes IO as an integrating concept that is a central portion of the MAGTFs combined arms approach. Additionally, the paper focuses on operational objectives that can enhance traditional combat power and explains that IO is continually conducted as a part of force protection. Moreover, the paper describes the need for IO service doctrine

that is integrated with the Marine Corps warfighting strategy of operational maneuver from the sea (OMFTS). Also addressed is the need to educate leaders regarding the importance of IO and ensuring actions are taken to secure Marine Corps information systems. The concept paper includes figure 3 which portrays the Marine Corps defined Elements of IO. These elements are in conjunction with joint IO doctrine with the exception of the additions of counter-reconnaissance and electronic protection. Joint doctrine lists EW as a part of DIO, but the Marine Corps concept paper does not. A review of joint IO doctrine is required to ensure a basic understanding of what is contained in the document. Further comparisons will be made between the Marine Corps concept paper and joint doctrine.

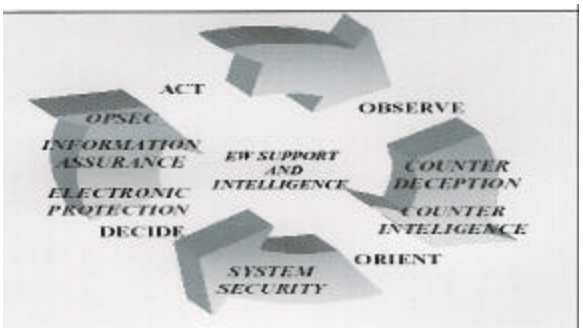

Figure 2. Defensive IO (MCDD 1998, fig. 4)

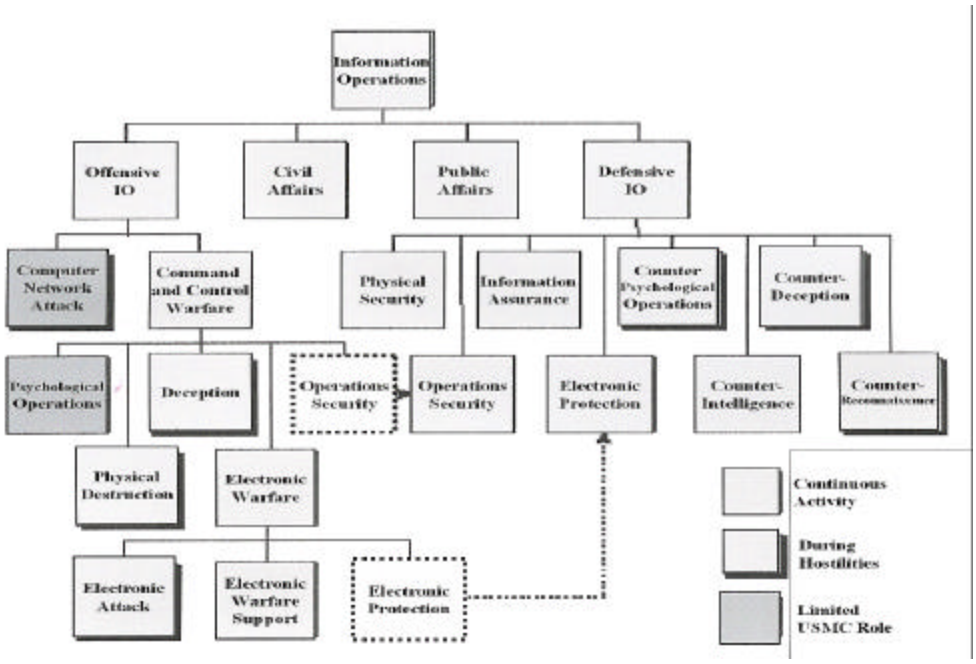

Figure 3. Elements of Information Operations (MCDD 1998, fig. 1)

The next portion of this literature review will focus on joint and service IO doctrine. The first publication reviewed is the Joint Publication 3-13 (JP 3-13), *Joint Doctrine for IO*. After a review of this publication, the Air Force and Army service doctrines will be reviewed.

Joint IO Doctrine

Joint doctrine for IO provides overarching guidance for IO in the context of joint operations. This document breaks IO into both defensive and offensive elements and describes the responsibilities related to each in joint operations. This publication is considered authoritative and as directed, will be followed in the conduct of joint operations. This document takes precedence over service doctrine should a conflict arise between the two. Chapter one of JP 3-13 begins by outlining the policy, responsibilities,

and terminology related to IO. Chapter two describes all facets of offensive IO to include principles and capabilities, range of military operations, IO and the levels of war, intelligence and information systems support, and targeting. Chapter three covers DIO and will be extensively used in writing this thesis. This chapter defines and describes DIO, information environment protection, IO attack detection, capability restoration, and IO attack or potential attack response. Chapter four describes the need for joint force IO organization and explains the relationship with joint activities and supporting DOD agencies. Chapter five explains the IO planning methodology and required coordination, integration and deconfliction, as well as providing guidance for IO input into the joint operation planning and execution system (JOPES). Chapter six is the final chapter and it describes IO in training, joint exercises, and how it can be used in modeling and simulation. This publication provides a framework for joint planners to work from when planning joint operations. It also provides the services with an outline of what IO tasks can be expected by a joint task force. This doctrine should be the driver for service doctrine to ensure they are in conjunction with the joint requirements.

Army IO Doctrine

The next IO doctrine to be reviewed will be the Army doctrine for IO, Field Manual 100-6 (FM 100-6). FM 100-6 begins by explaining that commanders must understand the new operating environment termed the global information environment (GIE). FM 100-6 describes information used on the battlefield as the military information environment (MIE) and discusses the interrelationships of the GIE and MIE. Figure 4 taken from FM 100-6 displays how this manual describes the GIE and MIE in relation to IO. FM 100-6 continues on with an explanation of the fundamentals of IO and how

IO must be integrated in military operations. The manual defines three types of military action that will enable a force to achieve information dominance. Those three elements are command and control warfare, civil affairs, and public affairs. This publication information systems on the modern battlefield. The final chapter of this manual is on planning and execution. This chapter describes the levels of war and the importance of IO at each level. Figure 5 is used in FM 100-6 to illustrate the employment of IO throughout the duration of a military campaign. This figure uses the three elements of information operations as defined in the FM 100-6 as relevant information and continues on to describe relevant information, intelligence, and the complexity of intelligence, information systems, and operations as the quantity of effort scale against the different phases of a military campaign along the bottom of the chart. This figure is the summation of the manual and describes the level of effort in relation to the military operation. As with most service doctrine this publication is far more detailed then the joint doctrine. Also, it uses Army doctrinal phrases, which differ from joint doctrinal phrases that on the surface make it appear that it is not in line with joint doctrine. After a review of both doctrinal publications, the basic concepts espoused by both are in concert. Therefore, military planners of other services could use this publication as a supporting reference when conducting IO planning.

Figure 4. Information Operations (HQDA 1996, fig 2-2)

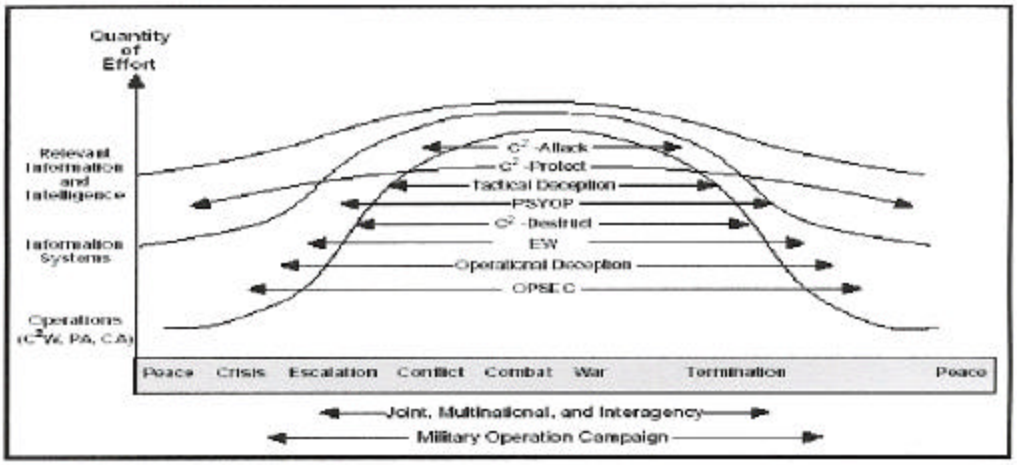

Figure 5. Employment of IO (HQDA 1996, fig 6-1)

Air Force IO Doctrine

The Air Force Doctrine Document 2-5 (AFDD 2-5) titled Information Operations, is written to focus on aerospace power and how information operations and information in operations are used to support aerospace functions. AFDD 2-5 takes a different focus then the Army publication, but the basic tenants described in this publication are in concurrence with joint and Army IO doctrinal publications. Chapter one of AFDD 2-5 looks at the nature of information operations. It discusses trends, threats and some of the considerations that must be made by military planners. Chapter two is titled "Counterinformation" and divides counterinformation into both offensive (OCI) and defensive (DCI) operations. The term counterinformation in this context, is the same as the term DIO and Offensive IO (OIO) used in this thesis. Table 1 displays the activities of DCI and OCI as presented in AFDD 2-5. Chapter three goes on to describe functions that support IO. In this chapter the roles of intelligence, surveillance and reconnaissance, precision navigation and positioning, weather services, and other support are discussed. Chapter four continues with a description of Air Force IO in the theater of operations. In this chapter the doctrine depicts an effects-based approach to IO. This chapter also discusses the strategic, operational, and tactical effects along with counterinformation planning, offense and defense integration, information warfare (IW) targeting, IW organizations and computer emergency response teams. Chapter five is the final chapter and provides a summary of the concept described in this publication. In summary, this publication uses the same basic concepts as the joint doctrine but with a focus on Air Force operations.

Table 1: Prominent Counterinformation Activities (HQ AFDC 1998, fig. 2.1)

Counterinformation	
Offensive Counterinformation	**Defensive Counterinformation**
Psychological Operations Electronic Warfare Electronic Attack Electronic Protection Electronic Warfare Support Military Deception Physical Attack Information Attack	Information Assurance Operational Security Counterdeception Counterintelligence Counterpsychological Operations Electronic Protection

Selected IO Works

The remainder of this literature review will focus on other selected works that pertain to DIO. Works pertaining to counterintelligence, counterdeception, counterpsychological operations, operations security, information assurance, physical security, and electronic warfare will be discussed.

The book *Intelligence Requirements for the 1980's: Counterintelligence* edited by Roy Godson is a collection of nine short papers relating to counterintelligence (CI). This book is considered as one of the most comprehensive unclassified works on counterintelligence published. Mr. Godson provides the introduction that outlines basic background information on CI. Although this book was published during the Cold War era, the concepts espoused in this publication are still relevant today. Godson defines CI in the following manner, "The identification and neutralization of the threat posed by

foreign intelligence services, and the manipulation of these services for the manipulator's benefit (Godson 1980, 1).

The second chapter of this book is a paper by Arthur A. Zuehlke Jr. titled *What is Counterintelligence?* In this paper, Zuehlke describes CI as basically a defensive function. He describes CI as a policing function within the intelligence community. He also refers to another author named Allen Dulles who describes the concept of CI information. He writes, "CI information is the "product" of counterespionage operations (Godson 1980, 15). Zuehlke goes on to describe CI with both passive and active components. He describes passive counterintelligence in the following way: "Passive counterintelligence seeks to counter potentially hostile, concealed acts . . . it comprises measures undertaken to protect against what adversary may do. Its function is essentially preventive and defensive. Typical of passive CI operations and activities are the following: (1) defensive source programs; (2) technical surveillance countermeasures (TSCM); (3) security education; and (4) estimating or assessing the vulnerability of sensitive installations and activities to the CI threat (Godson 1980, 26). Zuehlke describes active CI as detection. He describes the adversary intelligence services and their intelligence targets and collection operations. He emphasizes the importance of CI investigations. The following passage describes how he believes these investigations should be conducted: "CI investigations may be routine, aimed at identifying persons who are for various reasons vulnerable to entrapment or recruitment by a hostile service. Or these investigative activities may be aimed at the neutralization of personnel known to be in contact with or under the control of the hostile service. Both witting and unwitting agents are the targets of CI investigations" (Goodson 1980, 27-28).

Other papers in this book are written on counterintelligence organizations and operational security and how counterintelligence personnel can be recruited and trained. This book provides a comprehensive look at counterintelligence and should be read by any planners considering counterintelligence actions.

The next publication that will be reviewed is titled *Silent Warfare; Understanding the World of Intelligence*, by Abram N. Shulsky. This book describes various facets of intelligence. It begins by describing the scope and elements of intelligence. Chapter five of this book is on CI, which describes various aspects of CI. In this chapter an explanation of deception and counterdeception are also provided. This discussion of counterdeception is relevant to the content of this thesis. In this work, the author uses the historical example of the German World War II operation called Nordpol (North Pole). He explains that with deception, the more channels of information, the less likely a force will be deceived. He writes about the fact that the greater the dependence on one type of information the more vulnerable the force. Additionally, communication channels are vulnerable due to the fact that forces do not always know if foreign intelligence is gathering their data. "Even more important is the fact that the adversary will ordinarily be unable to tell which of his many communications channels others may be reading; he may well transmit fake messages that are never intercepted, while some real ones are. However, even this is not foolproof: via espionage or some technical means an adversary may learn on which frequencies or communications lines others are eavesdropping. If so, these communication channels might be used in a deception effort" (Shulsky 1991, 125). This book provides detailed insight into the intelligence community with many historical examples.

The next book to be reviewed is titled *Psychological Operations Principles and Case studies*, edited by Frank L. Goldstein. This book is a compilation of twenty-five short articles on Psychological Operations (PSYOP). These articles provide the reader with a thorough introduction into PSYOP. Many of the articles are written using historical examples to explain the power of effective PSYOP. These articles show how PSYOP reach from the strategic to tactical levels of warfare. Many of these articles explain that the goal of US PSYOP is to send a factual message. US forces use truth as the means to win favor over enemy populations and break the enemy's will to remain committed to their cause. This publication touches on many aspects of PSYOP to include counterpsychological operations.

Army regulation 530-1 Operations Security (OPSEC) published 3 March 1995 will be used, as a reference publication in the drafting of this thesis but due to the limited distribution requirement for this publication, will not be reviewed.

The subsequent review is that of a paper titled *Grand Strategy for Information Age National Security; Information Assurance for the twenty-first Century*, written by Kevin Kennedy, Bruce Lawlor, and Arne Nelson. This paper discusses the need for military strategy in the information age to better define the threat environment with which we live. They write about the new national security realities produced by dramatic technological changes. They also write about the fifth dimension of warfare being created by information technologies. The authors go on to describe the strategic framework where states derive their power from systems. They provide a brief illustration of how forces can be targeted in the information age and they show a framework to create a weapons-effects matrix. They continue with a discussion of

information centers of gravity and how those centers of gravity must be protected. In the end of this paper the authors write of the need for a strategic plan to deal with the new threats in the information age. The authors of this publication are senior military officers who provide insight from the years of their experience in the writing of this paper.

The following review is on the book titled *Cyberwars; Espionage on the Net,* by Jean Guisnel. This book provides a historical view of the expansion of the Internet. The author writes about the need for a government communication infrastructure in the event the world experiences a nuclear war. The book discusses many instances where people have used the Internet to exploit others and how the rapid expansion has opened up many people and organization to new vulnerabilities. The author writes about how the US government failed in their attempt to install a computer chip in all voice and data devices, which would have enabled government officials to decipher encrypted messages. This book is easy to read and provides many lessons learned for all users of data systems.

The following review is on the book titled *Cyberwar: Security, Strategy, and Conflict in the Information Age*, edited by Alan Campen, Douglas Dearth, and R. Thomas Goodden. This publication is a compilation of many short articles on IW issues. The book is written in four parts with part one covering the history of information warfare, part two covering cyberwar and civil society, part three covering how the US should organize for cyberwar, and part four covering warfare in the information age. This publication is one of the leading works published on the topic of IW. The articles in this book cover topics from strategic information warfare to ethical considerations that must be made when conducting cyberwarfare. This book should be read by all that study the topic of IO and IW because of the enormous amount of information that is covered by

these works. This book touches on most parts of IO and will be one of the main publications used in the development of this thesis.

The final publication that will be reviewed is *titled Network Centric Warfare; Developing and Leveraging Information Superiority*, by David Alberts, John Garstka, and Frederick Stein. This publication studies the information age and the affect on military operations. It includes a brief review of the changes that have occurred during the information age and how commercial organizations are driving many of the changes to information systems throughout the world. The book points out the fact that commercial organizations and competition are pushing systems to provide more accurate feedback and accountability. These improvements have created a situation where competitive awareness provides an advantage over others. The authors describe this awareness in relation to military operations. They show the need for friendly forces to have accurate and timely information to gain information superiority. They go on to describe the military as a network-centric enterprise. The book talks about the need for virtual collaboration of distributed staffs. The authors continue with a discussion of battlespace awareness and command and control issues. The book concludes with a discussion about the journey ahead for network-centric warfare. This publication provides a foundation for military planners to include network-centric warfare in the operational art of warfighting.

This concludes the literature review for this thesis. Many other works will be used in the drafting of this thesis, but were not as significant as those reviewed in this chapter. Chapter 3 will define IO and identify the IO threat.

CHAPTER 3

DEFINING IO AND ANALYZING THE THREAT

The purpose of this chapter is to define IO, DIO and to describe the IO threat to US forces. The primary works that this research will focus on will be *Joint Doctrine for Information Operations*, Joint Pub 3-13, 9 October, 1998, and *A Concept for Information Operations,* Marine Corps Concept Paper, 15 May 1998. These two works describe Information Operations from both joint and Marine Corps viewpoints. Additionally, a Master of Military Art and Science Thesis titled, *Marine Air-Ground Task Force Offensive Information Operations, Supporting Operational Maneuver From The Sea,* by Major Scott Aiken, USMC, will be used to ensure this paper is complimentary to this previous research. A review of Army and Air Force service doctrine will provide insight into how other services approach IO. This insight will be helpful but must be kept in context due to the differences between service doctrine and organization. Two other significant works, which will be used, are the Marine Corps Concept Papers, *Expeditionary Maneuver Warfare,* and *Operational Maneuver from the Sea.* These papers describe how the Marine Corps plans to operate during crisis situations in the future. These works focus on the new challenges of technology and how they will enable future Marine Corps Operations. These papers are the cornerstone of current Marine Corps doctrine development and will be extensively reviewed during this research.

The Marine Corps definition of IO as contained in MCO 3430.8, *Policy for Information Operations*, states, "Actions taken to affect adversary information and information systems while defending one's own information and information systems" (HQMC 1997, 2). This matches the definition published in Joint Publication 3-13, *Joint*

Publication for Information Operations. This definition differs with the Army and Marine Corps definition as defined in Field Manual 101-5-1 (Marine Corps reference Publication 5-1), *Operational Terms and Graphics*, which states, "Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an 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 capabilities" (HQDA and HQMC 1997, 1-82). Using these definitions as examples, one can see that even within the Department of Defense there is not exact concurrence on how to define IO. In the Marine Corps concept paper on IO, the author goes on to describe IO functions in the following manner:

> Marine Corps information operations (IO) support maneuver warfare through actions that use information in support of our National Military Strategy to deny, degrade, disrupt, destroy, or influence an adversary commander's methods, means or ability to command and control his forces and inform target audiences through informational activities . . . IO conducted by Marine Air Ground Task Forces (MAGTF's) will consist of battlespace shaping, force enhancement, and force protection activities. Information operations will enhance the ability of the MAGTF to project power during peace and war and will complement and facilitate the traditional uses of military force. (MCDD 2001, 1)

The paper also states that IO is an integrating concept that enhances warfighting functions. The concept paper primarily focuses on command and control, fires, maneuver, logistics, intelligence, and force protection as those warfighting functions supported by IO. The USMC concept paper further describes IO in the following context: "It is not simply another 'arrow' in the MAGTF commander's quiver. It is, rather, a broad-based integrative approach that 'makes the bow stronger.' Thus, the focus

of Marine Corps IO will be upon the information-oriented activities that will best support the tailored application of combat power" (MCDD 2001, 1). The concept paper continues on to describe the offensive and defensive elements of IO. It describes offensive IO as being the primary IO focus at the operational and tactical levels of war, "A principal focus of 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 and destroy his military operational effectiveness. Integrated targeting to achieve the desired operational effects will combine influence, information, and weapon effects to shape the physical, electronic, and informational aspects of the battlespace" (MCDD 2001, 8-9). Furthermore, the paper states, "the MAGTF may rely on national-level agencies and other service components for certain offensive IO-related capabilities - to include computer network attack, psychological operations, and the means to manage media attention on the operation" (MCDD 2001, 9). The concept paper provides a more detailed description of DIO. The paper breaks DIO into four interrelated processes: "information environment protections, attack detection, capability restoration, and attack response" (MCDD 2001, 9). While each of these processes is related, each requires unique skills to execute. The following provides a brief overview of each of these DIO elements.

Using command policies, procedures, and technologies to guarantee freedom of action in the information environment help to achieve information environment protection. This protection is gained by managing risks to ensure that information systems are safeguarded. In this protection role, operational security (OPSEC), is always given consideration, because weak OPSEC creates vulnerabilities to the best defenses.

The need for OPSEC is also weighed with that of military deception, public affairs and psychological operations.

In addition to needing to protect the information environment, the MAGTF must also have an attack detection capability. The Marine Corps concept paper on IO states that, "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" (MCDD 2001, 10). The MAGTF also requires a capability restoration in relation to their information systems. They must ensure that information systems are designed with redundancy and resilience to withstand effects of environmental phenomena as well as enemy actions. Redundant capabilities must be built into all critical elements of an information system.

In addition to the three aforementioned capabilities, the MAGTF also requires an attack response capability. This will provide the MAGTF commander with the ability to respond to attacks on his information systems. His responses may be either passive or active depending on the situation. If using active measures, he will seek to destroy or degrade the adversary's attack capability. If he is using passive measures, he will attempt to mitigate the effects of the adversary's actions.

Using these criteria for DIO, a review of the vulnerabilities and threats is required to better understand how these interrelated activities should be conducted by the MAGTF. Understanding friendly vulnerabilities and developing protections for them is a fundamental element of defensive military operations.

Since the world has changed so drastically in the past twenty years with the fall of the Soviet Empire and the explosion of communication technology, identifying the IO threat has become increasingly complicated. Joint Pub 3-13 describes some of the vulnerabilities to US information and information systems. This description explains that due to the multimedia world, there are many forms of information. Information can be stored on computer disks, videos, written forms such as letter, books, and files. The task of securing these multiple means of communications is enormous. Additionally, the description of information systems looks at three main elements of all information systems. These three elements are human factors, communication or network nodes, and links into the communication nodes. Because of the complexity and global nature of networks, it has become increasingly difficult to defend against information attacks.

Human factors must be considered and involve not only the direct attack of an information system from an enemy outside of the military organization, but also include the insider threat. Disgruntled employees and those that may be sympathetic to the enemy cause, can be the worst kind of threat because they are treated as trusted individuals and granted access to the military information systems. This insider threat requires continued background checks and command oversight to ensure all who are granted access to military information systems are at a low risk for insider sabotage. The outsider threat can come in many forms as well. The outsider can be a hacker who attempts to enter information systems via unauthorized means, by either obtaining the passwords or computer code to enable access to information systems. The outsider could also be an individual who through whatever means, is able to disrupt or destroy an information system without directly accessing the system. An example of this would be

to take down a power grid that supports information systems. This would deny users access to their systems while the attacker never attempted to break into the information systems. This type of attack, coupled with a natural disaster such as a severe storm, may make it difficult to identify that an attack had actually occurred. The human factors are so diverse and complicated that they are the most difficult to assess and protect against.

Another type of vulnerability rests with the communication nodes. These nodes can reach from the tactical world all the way to the strategic. Key switching centers and network routing facilities can be targeted because they link the military operations into the DOD global information grid (GIG). These nodes are a part of the communication backbone, when if destroyed or disrupted, can have a far-reaching effect (means to an end) on the deployed military communications system. The nodes include both satellite and terrestrial communications facilities. These nodes are typically in a static environment for long periods of time and most are owned by commercial sources. Network nodes are considered the nerve centers of the network. They route voice, video, and data throughout the network. Because of the static nature of these nodes, they are vulnerable to attack.

The third set of vulnerabilities is found in the communication links. These are connections from communication nodes to the end user. Links can be cell phone connections, remote satellite terminals, telephone connections, and local area network connections. Since links are a localized capability, attacking them may have limited results. But by attacking only one link and not an entire node, the victim of the attack might not be able to identify that they are in fact being attacked. In this situation the system as a whole appears to be working properly and other users are successfully using

the system. If an individual link is attacked, it might appear as a localized malfunction rather than an attack. This type of attack is generally more difficult to execute because safeguards and monitoring devices have been built into most nodes to protect their end users. Links are generally more susceptible to insider attack because the attackers have access to the system.

Understanding these vulnerabilities is important, but still requires an understanding of the enemy threat. To understand the threat to Marine Corps information, a review of the Marine Corps concept paper on IO is an appropriate starting point. The concept paper describes the threat in these terms, "Threats to the information infrastructure come from those motivated by military, political, social, cultural, ethnic, religious, economic--and even personal gain. The globalization of networked communications creates new vulnerabilities, as does the world's increasing dependence upon high volumes of timely, accurate information" (MCDD 1998, 3). Since MAGTF's are deployed around the globe, they will be exposed to many threats. These threats will come in many varieties and will pose new and ever changing hazards even during times of relative peace.

The mere use of information technologies can be viewed as a threat. These technologies when improperly used can contribute to information overload, micro-management and the illusion that certainty and precision in war is attainable. Additionally, command and control systems are vulnerable to physical destruction, exploitation or disruption via spoofing, misinformation, hacking, jamming, and other means. The imprudent uses of information technologies provide the enemy with new opportunities. These opportunities are gaps that allow the enemy to penetrate our defenses. The Army Field Manual 100-6,

Information Operations, provides a detailed description of the IO threat. It states: "the threats to the information infrastructure are genuine, worldwide in origin, technically multifaceted, and growing. They come from individuals and groups motivated by military, political, social, cultural, ethnic, religious, or personal/industrial gain. They come from information vandals who invade INFOSYS [information systems] for thrill and to demonstrate their ability" (HQDA 1996, 1-5). This description continues on to explain that due to globalization of the communication networks and increased access to these networks from virtually any location in the world has created numerous vulnerabilities to military information. This field manual uses the figure 6 to describe the level of hostility from peacetime to war by the technical capabilities and motivation of the attacker. These threats run from the tactical to strategic and come from a variety of sources. The threat is always present, even during times of relative peace. The field manual uses the following examples of options available attacking information systems and services. It states that attacks can be immediate, such as the physical destruction of an information system, or they can be delayed, as with the introduction of a computer virus or logic bomb that executes at a certain time (HQMC 1996, 1-6). Each of these methods is effective in denying the use of a particular information system. Other means of information attack come from unauthorized access to either insert data into the system or to retrieve data from the system. Introducing a program that enables the bypass of network defenses can be an effective method of gaining access to sensitive information. These programs can be emailed to a legitimate user and then upon opening the email or attachment, the hidden program executes without the user's knowledge. Likewise, the corruption of data or electronic attack (EA) can make data misleading or useless to the

user. The most common forms of EA are the broadcasting of false signals and jamming. Additionally, the collection of signals, radiation and data, can be used as electronic intelligence. Lastly, the use of deception and psychological operations (PSYOP) can influence friendly information systems.

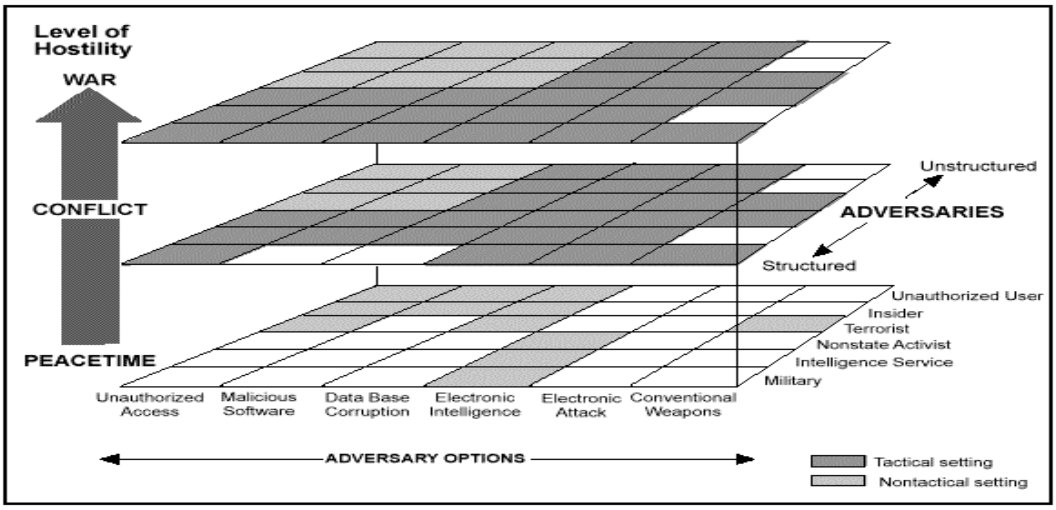

Figure 6. Threats to Information Systems (HQDA 1996, fig. 1-2)

These measures can be used to cause a loss of confidence in information systems and alter or damage the integrity of the data. This in turn, can lead to a lack of trust and can cause the military user to either not use a system or to minimize its use. Regardless, the enemy can cause a degrading effect on these systems by employing the aforementioned measures.

As previously mentioned, the threat can come from many sources. Unauthorized users, insiders, terrorists, non-state groups, foreign intelligence services, and opposing political or military opponents, must all be considered when analyzing threats and

motivations for attacks on information systems. The two groups that have significant impact but are difficult to pinpoint, are the terrorists and non-state groups. Terrorists and non-state groups cross international boundaries and are not easily identified. Terrorist use direct attacks to cause a drastic effect, which they hope will have a psychological effect on their target. Terrorists employ commercially procured information systems for their information attacks. The global information networks provide a means for terrorists to coordinate worldwide activities. Terrorist groups, who use computer bulletin boards to pass technical data and intelligence, can easily cross international borders. Additionally, non-state organizations such as organized crime and fundamentalist religious fanatics, are taking advantage of information systems. They use commercially procured encryption to protect their information and since they are spread throughout the world, they use the global information infrastructure to pass data. These groups hire skilled hackers to attack opponents and use information technologies to shape public opinion regarding their cause. These non-state actors attempt to use the media as a platform to sway public opinion.

Another potential attacker comes from the foreign intelligence community. These agents will use anonymity via Internet chat rooms and billboards to collect data. These agents primarily target commercial networks and scientific institutions to gather data. Their secondary focus would be direct military information. Hiding amongst the millions of computer users enables the foreign agent the anonymity he desires in the execution of his duties.

Furthermore, political actors and opposing military adversaries use information systems such as the media to manipulate public opinion to further their aims. These

opposing actors use television, radio, and Internet web pages to push their agendas. This media effort must be treated as a serious threat, because it enables these parties to portray friendly forces in a harmful manner thus rallying support for the opposition. A thorough understanding and embracing of the free press is important to counter this threat.

Threats to information systems evolve as a crisis grows to conflict. In peacetime the threats of unauthorized access and the distribution of malicious software are the greatest threat. As a crisis evolves into wartime conflict, the IO attacks become more direct. During wartime, attackers will target individual units and their supporting information infrastructure, and will exploit the vulnerabilities that were discovered during peacetime. Intrusions and insertions into military networks will enable the opposing force to embed malicious software to disrupt communications on those networks. Field manual 100-6, *Information Operations*, states that,

> On the battlefield, reliance on an extensive and potentially fragile communications infrastructure presents a vulnerability that entices exploitation. The initial candidates for attack could be vital information nodes or links such as CPs [command posts] and communications centers. In addition to striking battlefield information nodes, adversaries can also strike the supporting infrastructure, both on and off the battlefield. Central system support assets such as power sources can be very difficult to repair or replace. Artillery, tactical ballistic missiles, and air power provide the major attack systems for most adversaries today. (HQDA 1996, 1-7)

Strike capabilities will continue to grow as the proliferation of powerful weapons systems persists. Weapons proliferation include cruise missiles, precision guided missiles, chemical and biological contaminants, and nuclear weapons. Additionally, the spread of global positioning systems using satellite technologies have produced very accurate weapons delivery systems. Recognizing that these technologies are inexpensive to purchase and easily obtained by any adversary is a must.

The last threat that will be discussed is that of natural phenomena. This includes situations where natural disasters disrupt or destroy information systems. The occurrence of a hurricane or a tornado that rips through a headquarters compound can have a devastating effect on the headquarters and provide an opportunity for an adversary to exploit. It is during times of natural disaster that military IO personnel must be mindful of the effects of natural phenomena on the network restoration process. Military personnel must not be confused with the outage that was caused by a weather event and those that may have been caused by an adversary who is using the weather event to cover their actions. Although these events may not be common, adversary forces may have developed an attack and are just waiting for the opportunity to piggyback onto a major weather disaster. If not caught, this type of attack can cause confusion during the restoration process. This is yet another threat to US information that must be considered by military planners.

This chapter has defined IO, DIO, and the threat to US IO. This chapter demonstrated that the IO threats are endless. A continued focus on the IO threat is required for successful IO in the future. New information capabilities are continually being fielded. While these new technologies provide tremendous capabilities, they also introduce new vulnerabilities. It will often take many years of using systems to understand all of the faults that may have been built into the system. This means that just as our forces think they have a handle on the threat, new threats are being developed daily. This is something to consider when introducing new systems during military operations. In the next chapter, this thesis will review current Marine Corps DIO capabilities to meet these IO threats.

CHAPTER 4

MAGTF DIO CAPABILITIES

This chapter will review current Marine Corps DIO capabilities. Each aspect of DIO will be examined to determine the Marine Corps' ability to conduct these operations. If no current Marine Corps capability exists, then the means for obtaining that capability will be reviewed. This review will focus on the following elements of DIO: information assurance, physical security, operations security, counterintelligence, counterdeception, counterpsychological operations, and electronic warfare. The intent of this chapter is to provide the reader with a brief understanding of current MAGTF DIO capabilities.

Information Assurance (IA)

In recent years, IA has been the main focus for the data communication community. The technicians that provide network access have been implementing various defensive measures to protect friendly information from collection, corruption, or denial. Due to a large push by DOD leadership, IA has become a commonly known term to many military personnel. To ensure the term is properly understood, the following definition will be used, "IA protects and defends information and information systems by ensuring their availability, integrity, identification and authentication, confidentiality, and nonrepudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities. IA employs technologies and processes such as multilevel security, access controls, secure network servers, and intrusion detection software" (CJCS 1998, III-1). These elements of IA are depicted in figure 7. The figure depicts a key representing a user's access to a computer network.

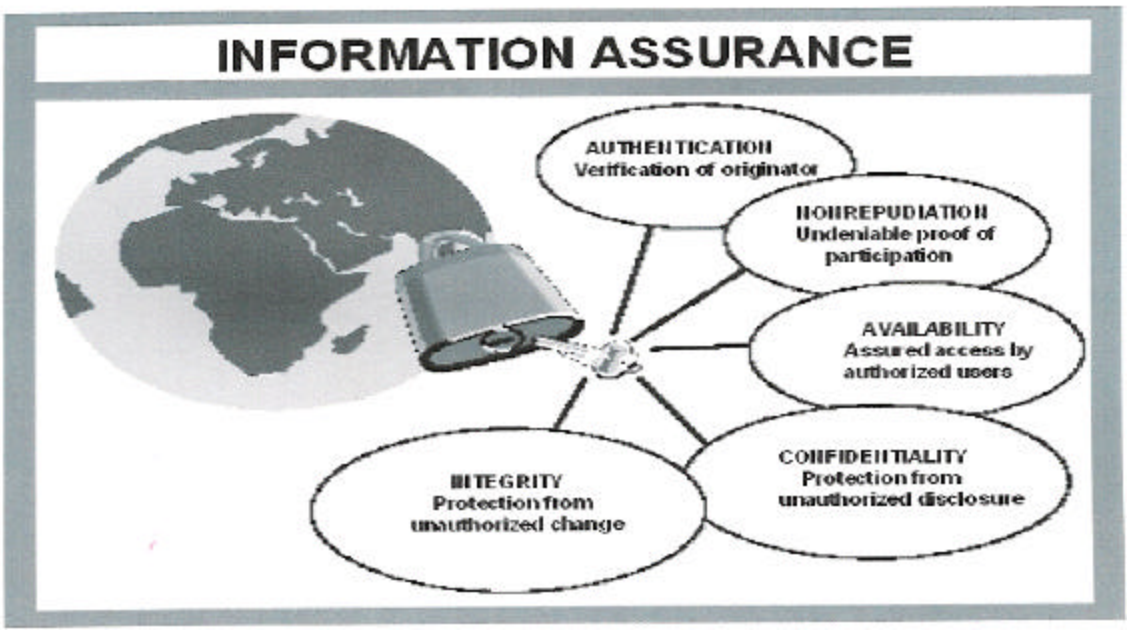

Figure 7. Information Assurance (CJCS 1998, fig. III-2)

The key is made up of several elements of IA. To better understand each facet of the key, one must first understand the definition of each element. The first element that will be reviewed is that of authentication.

> Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of log on passwords. Knowledge of the password is assumed to guarantee that the user is authentic. Each user registers initially (or is registered by someone else), using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The weakness in this system for transactions that are significant (such as the exchange of money) is that passwords can often be stolen, accidentally revealed, or forgotten. (Gagne 2001, 1)

The Marine Corps currently uses password authentication for computer network access. While password authentication provides a measure of security for a computer system, as stated above, it is vulnerable to being discovered by unauthorized persons. If an unauthorized person discovers an authorized user password, then they can gain access

into the system. Additionally, password-cracking software can be purchased on the commercial market place and can be used to enable a person to see another person's legitimate password. "Your password-protected PCs and data files aren't nearly as secure as you might think. Software that can detect your passwords is readily available. You may think that such programs are the sole domain of computer crackers and unscrupulous users--but that's not the case. Instead, password-cracking utilities tend to be marketed primarily for the legitimate purpose of helping administrators recover lost passwords. In the wrong hands, however, such programs can easily compromise your system's security" (Seltzer 2001, 1). Due to the vulnerability of network passwords, the Department of Defense (DOD) has begun implementing a physical access card for network authentication. Built into the card is a digital identification code called an electronic signature. The electronic signature is stored on a computer microchip, which is imbedded on the user identification card. This signature provides a unique identification for an individual user. These new identification cards are part of a DOD program called the common access card (CAC). The CAC is described in the following manner:

> The Department of Defense (Department or DoD) is implementing smart card technology as a Department-wide Common Access Card (CAC). A smart card is a credit card size token with one or more embedded memory and/or microprocessor integrated circuit chips (ICC). The CAC also contains a linear barcode, two-dimensional barcode, magnetic stripe, color digital photograph, and printed text. The CAC will be the standard identification card for active duty military personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. The CAC will also be the principal card used to enable physical access to buildings and controlled spaces and for logical access to the Department's computer networks and systems. The CAC ICC has a cryptographic co-processor to enable it to serve as a token for the PKI identity, email, and encryption certificates. (DOD Access Card Office 2001, 1)

In this description PKI means public key infrastructure, which is another DOD-wide program. An overview of the program is appropriate, " Many programs supporting the Department of Defense (DOD) missions require security services, such as authentication, confidentiality, non-repudiation, and access control. To help address these security problems, the DOD developed a Public Key Infrastructure (PKI). The DOD provides products and services that enhance the security of networked information systems and facilitate digital signatures" (DISA 2002, 1). It is through this PKI program that military members will receive their digital signatures for use with the CAC. This smart card will make electronic signatures the preferred method of verifying user identity when they attempt to access military computer systems. Since the verifying data is stored on the person's smart card, the user maintains physical control of their own electronic signature data. This capability is currently being fielded throughout DOD. The Marine Corps is part of the Department of the Navy (DON) CAC program and has already begun fielding this technology.

> By the end of FY 02, over 1.1 million Smart Cards will have been issued to active duty, selected reserve, civil servants and selected contractors. Implementing the Smart Card throughout the DON will take much effort and dedication by all personnel to effect the physical and cultural changes required. However, with the dedication to excellence of Navy and Marine Corps personnel, impressive technology applications and effective knowledge management, the implementation of Smart Card will bring about a positive global change for the DON. Smart Cards will be 'your passport to the e-world.' (Hyers 2000,1)

The DOD realizes that the CAC is still vulnerable to theft so they have also coupled the card with a personal identification number and a network password which will provide multiple layers of protection. This program provides the greatest measure of assurance available with current technology.

In addition to providing authentication for users on a military network, the CAC also provides undeniable proof that a particular user sent information over the network. This undeniable proof is called nonrepudiation. "Nonrepudiation is the ability to ensure that a party to a contract or a communication, cannot deny the authenticity of their signature on a document or the sending of a message that they originated. On the Internet, the digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature" (Gagne 2001, 1). This nonrepudiation ability is important due to the insider threat to military information. This threat exists because a legitimate user could send military information to an unauthorized party. The ability to prove that a particular user sent this unauthorized communication is vitally important. All DOD components must have this accountability to help minimize the insider threat and to punish any violators. While nonrepudiation is effective, it is not foolproof; users could leave their workstations unattended and logged on with his CAC inserted. This would provide another user the ability to assume control of the unattended workstations and use the identity of the absent person, to send information over the network. Although the CAC is not foolproof, it does provide a better degree of security to protect one's identity when coupled with other authentication methods. Through thorough user training, the threat of one user using another's log-in password, personal identification code and CAC is minimized. The Marine Corps is currently providing user training to ensure the validity of the nonrepudiation portion of the CAC program.

The next aspect of the IA is the availability of access to required information systems. As mentioned previously, this is another function that will be built into the CAC. The CAC will provide network access to any authorized Marine Corps user anywhere in the world. To gain access, the user will simply log into a networked machine by inserting their CAC into a card reader and then enter their PIN and password. Military networks will be designed to recognize authorized users and approve access to these systems. This will provide access to users that come together from various units to form a MAGTF, the ability to quickly access the network without having to change their network identity. The timeliness and ease of access will also increase the flexibility of Marine Corps networks supporting the MAGTF.

Confidentiality is another element of IA. It is described by joint doctrine as the protection from unauthorized disclosure. As a part of the aforementioned PKI program, the Marine Corps is currently adopting new technologies to encrypt email. The encryption of email provides the users with a secure means of transferring information over the Internet. This technology will ensure that information remains confidential and can only be accessed by the intended recipient. This encryption capability will be built into the CAC so that user's email can be secure. The PKI system has been proven to provide secure communications over the Internet. The Marine Corps is currently in the process of fielding their own PKI capability.

In addition to the confidentiality gained by protecting email from unauthorized disclosure, the PKI encryption also provides for data integrity. One of the threats to information transfer over a network is interception. The intercepted information could then be modified and sent to the legitimate recipient or destroyed. This interception of

military information could lead to disaster during military operations. This is where nonrepudiation is important to ensure the identity of the person sending the data. Since the integrity of the data is vitally important, the PKI system was designed to provide protection against unauthorized access to US military information. Data will not be easily accessed because of the strong encryption capabilities of the PKI system. Therefore, once the PKI system is fully fielded throughout DOD, the threat of unauthorized manipulation of information will be minimized. This will ensure that information sent to a legitimate user will arrive intact and as intended by the sender.

Additionally, the Marine Corps has implemented security measures on their networks, which prevent unauthorized access to their systems. The Marine Corps has published detailed guidance on the use of virus scanning software that provides protection from the corruption of data. All Marine Corps networks are protected with virus scanning software. " Much of the success of the Information Systems Management Office (ISMO) team comes from educating the Marines on these dangers and keeping them up to date with the latest virus software. Weekly updates for virus software are installed on every machine on the network" (Perkins 2000,1).

Also, the Marine Corps has installed firewalls and intrusion detection software on their networks that limit and monitor access into and out of a network. "All DOD information will be protected from unauthorized users by proper employment of approved firewalls and associated intrusion detection software . . . firewalls have been installed throughout the Marine Corps" (HQMC 1999, 1). These firewalls block unauthorized computer programs or Internet addresses from entering the network. Additionally, the intrusion detection software records attempts by Internet addresses

outside of the Marine Corps network that try to gain access to the network. This provides the Marine Corps network managers with the addresses of unauthorized parties that have attempted to gain access to the Marine Corps system. This device, working in conjunction with the firewall and virus scan software, provides the Marine Corps networks with a great measure of protection. The enforcement of strict security policies has provided the Marine Corps with better protection from a network attack.

All of the previously mentioned elements of IA are important to the MAGTF's ability to conduct military operations. As is stated on the Headquarters Marine Corps Command, Control, Communications, and Computers (C4) department webpage, "Information Security is 'THE' critical weapon to combat the Marine's threat to his Command, Control, Communications and Computers. Attack C4 and you attack the Marine Corps' nervous system. Guard it, patrol it, protect it . . . and you protect the Marine protecting our country" (HQMC 2001a, 1).

Physical Security

The next element of DIO is physical security. The security of military personnel, facilities and equipment is a key concern for military planners. This element of security is termed physical security because it is the implementation of physical measures for security. Joint Pub 1-02 (JP 1-02) defines physical security as: "That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against espionage, sabotage, damage, and theft" (CJCS 2001, 327). Using this definition, it may become apparent that physical security is a task well suited for the Marine Corps. The history of the Marine Corps is full of examples where Marines

were assigned to safeguard personnel or guard installations, equipment, material, and documents from potential adversaries. The task of physical security in relation to DIO refers to the security of those key leaders, facilities or systems that are vital to the success of a military operation. JP 3-13 states, "Defensive IO integrate and coordinate protection and defense of information and information systems (which include C4 systems, sensors, weapon systems, infrastructure systems, and decision makers). Defensive IO are an integral part of overall force protection" (CJCS 1998, III-1). The ability to physically secure such systems and personnel require a trained force that is equipped for the mission. This security capability is stated in the official mission of the Marine Corps, which came from the National Security Act of 1947, amended in 1952. "Provide Fleet Marine Forces with combined arms and supporting air components for service with the United States Fleet in the seizure or defense of advanced naval bases and for the conduct of such land operations as may be essential to the execution of a naval campaign . . . Provide detachments and organizations for service on armed vessels of the Navy and security detachments for the protection of naval property at naval stations and bases" (Marine Corps TECOM 2002, 1). Since these defensive capabilities are written into the Marine Corps mission, the Marine Corps must train and equip their force to meet these requirements. In addition, the Marine Corps has also been given the task to provide security teams for American embassies. The Marine Corps has become recognized for its ability to act as a security force. Physical security is one mission that the Marine Corps is prepared to execute.

Operations Security

The next element of DIO is OPSEC. OPSEC is defined as, "A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation" (CJCS 2001, 313). As the definition states, OPSEC is the security of information about military operations and activities. The challenges with OPSEC are many. Military operations, exercises, and movements are often difficult to conceal. The knowledge gained by gathering such information about military activities can provide adversaries with the information they need to impact such activities. In this modern day, where communication devices are readily available around the world, the use of unsecured email and telephones create a vulnerability to US forces. An adversary can intercept these unsecured transmissions and use them to exploit and gain an advantage. Additionally, the fact that many military personnel and leaders travel with laptop computers and personal data devices is another concern. These personal devices are used to store critical data about their involvement in military activities thus creating an operational security vulnerability. Securing these portable systems has become just as critical to military information as the sentry standing guard at the entrance to a military installation. OPSEC can also encompass such actions as ensuring that both classified and unclassified documentation is properly destroyed prior to disposal. If such documents are

not destroyed, adversaries can gather the documents from the trash exposing friendly military information. The Marine Corps understands this problem and on 18 September, 2001, the Commandant of the Marine Corps, published a message titled: *Information (INFOSEC) and Operations Security (OPSEC) Reminder*. This message was sent to all Marine Corps commands and was posted on the official Marine Corps website. This message states the following reminders in relation to OPSEC, "We must be aware that our adversaries have the capability to actively monitor our communications, the news media, the Internet and command information channels . . . Casual conversations about sensitive information or speculation about operational matters in public venues can be exploited. Individuals must be cognizant of their surroundings at all times when discussing operational matters" (HQMC 2001b, 1).

The message goes on to provide guidance on how Marines should secure their operational information. While the Marine Corps is taking steps to educate Marines about the OPSEC threat, the vulnerability will always exist. As long as Marines use unsecured methods of communication they will be vulnerable to unwanted interception. The challenge to OPSEC lies in training Marines so that they understand the impact of leaked information. The loss of information from improper OPSEC can give the adversary an unwanted advantage.

Counterintelligence

The next element of DIO that will be reviewed is counterintelligence (CI). According to Marine Corps intelligence doctrine, there are two primary objectives of intelligence. The two objectives are:

> First, it provides accurate, timely, and relevant knowledge about the enemy (or potential enemy) and the surrounding environment . . . The second intelligence objective is that it assists in protecting friendly forces through counterintelligence. Counterintelligence includes both active and passive measures intended to deny the enemy valuable information about the friendly situation. Counterintelligence also includes activities related to countering hostile espionage, subversion, and terrorism. Counterintelligence directly supports force protection operations by helping the commander deny intelligence to the enemy and plan appropriate security measures. (HQMC 1997b, 5-6)

This publication demonstrates the Marine Corps' recognition of the important role counterintelligence plays in military operations. Additionally, a review of the Marine Corps Order (MCO) P1200.7W, *Military Occupational Specialties (MOS) Manual*, outlines the desired CI skills required of intelligence officers and CI enlisted Marines. According to this order, the Marine Corps assign the MOS of 0204, Human Intelligence (HUMINT) Officer to those officers trained in both HUMINT and CI. This manual describes the duties of the HUMINT officer as a: "Human source intelligence (HUMINT) officers serve in both counterintelligence (CI) and HUMINT billets. Duties include serving as CI platoon commander, Interrogation (IT) platoon commander and company executive officer within the HUMINT Company as well as serving as a division or MEF [Marine expeditionary force] staff officer" (HQMC 2001e, 22). This manual also outlines the training requirements for the HUMINT officer and states that these officers must complete the MAGTF Counterintelligence Course or the MAGTF Counterintelligence Reserve Course. The Marine Corps has Warrant Officers (WO) who specialize in counterintelligence. These WOs hold a MOS of 0210, Counterintelligence Officer. The duties of these CI officers are described in the following manner:

> serve in both CI and HUMINT billets. They conduct technical surveillance counter measures (TSCM), provide expertise in advanced foreign CI, and advise

> tactical commanders in force protection operations. Duties include serving as a CI assistant platoon commander and HUMINT Exploitation Team (HET) Commander within the HUMINT Company, service on a MEF staff, Naval Criminal Investigative Service, and serving as a CI representative to unified commands and national-level agencies. CI limited duty officers function as supervisors, advisors and coordinators of counterintelligence activities and human intelligence collection include serving as CIHO [counterintelligence/human intelligence officer] at the MEF or MARFOR [Marine forces] headquarters, service with the Naval Criminal Investigative Service, serving as staff officers within the CI/HUMINT Branch, HQMC, and serving as a CI representative to national-level agencies. (HQMC 2001e, 25)

These CI officers are specialists in the field of CI. As is apparent from the scope of their duties, these WOs can be found at all MAGTF and higher headquarters commands. In addition to the aforementioned officers, the Marine Corps also has enlisted personnel trained as CI specialists. These Marines are assigned the MOS 0211. The 0211 Marine performs the following duties:

> They are involved in all facets of planning and conducting tactical CI and human intelligence operations and activities. These activities are designed to locate, identify, and neutralize hostile intelligence and terrorist threats to the command. A collateral duty for CI specialists is to conduct human intelligence operations to collect information of intelligence value to the commander. In support of these functions, CI specialists utilize automated databases interview/interrogation techniques, liaison, specialized CI techniques, technical support measures, intelligence/investigative photography, report writing techniques, and other capabilities as required to accomplish the mission. CI specialists are expected to possess a working knowledge of the organization, operations, and techniques employed by foreign intelligence services and terrorist organizations. CI specialists normally perform as members of a CI subteam, detachment, or HUMINT Exploitation Team (HET). (HQMC 2001e, 25)

In addition to training these CI Marines, the Marine Corps participates in a program called Foreign Counterintelligence program (FCIP). "The FCIP provides Marine Corps participation in DON counterintelligence activities through the Naval Criminal Investigative Service (NCIS)" (HQMC 1997a, 90). Marine Corps involvement with the NCIS provides the Corps with the following capabilities: "Counterintelligence Force

Protection is the NCIS response to this threat . . . the NCIS collects and analyzes information about possible threats from various sources and advises military commanders on how best to defend against them. This requires NCIS personnel to work closely with the planning staffs of the operational forces they support, while other NCIS personnel must be forward deployed, acting as the eyes and ears for the approaching forces" (NCIS 2002, 1). This forward-deployed capability of the NCIS provides the Marine Corps with the ability to better plan for the environments and situations that they can expect to be deployed. In addition to these assets, the MAGTF can request CI assistance from other US intelligence activities. This assistance, along with the trained CI personnel on their staff, provides the MAGTF commander with a credible CI capability.

Counterdeception

The next element of defensive operations that will be reviewed is counterdeception. Counterdeception is defined as: "Efforts to negate, neutralize, diminish the effects of, or gain advantage from a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations" (CJCS 2001, 101). To fully understand this definition, the reader must first understand what is meant by deception in the context of a military operation. US Joint doctrine defines military deception as: "Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission" (JP 1-02, 2001, 266). The joint definition describes military deception in five categories: strategic military deception, operational military deception, tactical military deception, service military

deception, and military deception in support of operations security (OPSEC) (CJCS 2001, 266). Each of these types of military deception is defined as follows:

> Strategic military deception- Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and actions that support the originator's strategic military objectives, policies, and operations. (CJCS 2001, 266)
>
> Operational military deception- Military deception planned and executed by and in support of operational-level commanders to result in adversary actions that are favorable to the originator's objectives and operations. Operational military deception is planned and conducted in a theater to support campaigns and major operations. (CJCS 2001, 266)
>
> Tactical military deception- Military deception planned and executed by and in support of tactical commanders to result in adversary actions that are favorable to the originator's objectives and operations. Tactical military deception is planned and conducted to support battles and engagements. (CJCS 2001, 266)
>
> Service military deception- Military deception planned and executed by the services that pertain to service support to joint operations. Service military deception is designed to protect and enhance the combat capabilities of service forces and systems. (CJCS 2001, 266)
>
> Military deception in support of operations security (OPSEC) — Military deception planned and executed by and in support of all levels of command to support the prevention of the inadvertent compromise of sensitive or classified activities, capabilities, or intentions. Deceptive OPSEC measures are designed to distract foreign intelligence away from, or provide cover for, military operations and activities. (CJCS 2001, 266)

Using these definitions, it becomes apparent that the ability to use military deception at all levels of war is the responsibility of commanders. Since MAGTFs are often deployed around the globe during peace and wartime, they can be used as a deception tool at all levels. The MAGTF planners should use these elements of deception to better understand how their adversaries might attempt to execute military deception against the US This will enable the planners to build a viable counterdeception plan to negate any advantage the adversary attempts to gain. MAGTF planners must attempt to use these

deception operations to counter an adversary's deception plan. The MAGTF deception could result in the adversary believing that their deception plan is actually working. The MAGTF must rely on their military intelligence personnel to identify the potential adversary deception plans. This information on adversary deception plans can then be used to develop friendly force measures to negate that plan. The Marine Corps has incorporated deception planning as a part of the Marine Corps planning process. This process is outlined in the Marine Corps Warfighting Publication 5-1. The purpose of this publication is stated as the following:

> describes a planning process that supports decision making by the commander. It is also a vehicle that conveys the commander's decisions to his subordinates. It is applicable to all echelons of command and across all ranges of military operations . . . The Marine Corps Planning Process (MCPP) complements joint deliberate and crisis action planning and the naval planning process. It is a responsive and flexible process that can adapt to the needs of any size unit and adjust to any timetable. The Marine Corps planning process embodies our maneuver warfare doctrine with its tenets of top-down planning, single-battle concept, and integrated planning in order to generate and maintain tempo. (HQMC 2001f, Foreword)

Appendix G of this publication is titled Basic Operation Plans, Operation Orders, Annexes, and Appendices. In this appendix, there is a description of how to write the military deception portion of an operation order. The Marine Corps military deception plan can be found under Tab A to Appendix 3 to Annex C of an operation order (HQMC 2001f, G-48). Within this plan, listed under the heading of enemy general capabilities, is a description of the enemy's capabilities to conduct deception operations. Additionally, listed under Exhibit 2 to this Tab, the Marine planner will be asked to provide information on enemy deception and denial activities: "Provide an analysis of the targeted country's use of deception and denial in support of its political and military goals. Identify the target's deception and denial methods and current deception and denial

activities“ (HQMC 2001f, G-54). The publication continues to ask the Marine planner to determine the target’s reaction to military deception. In exhibit 2, the planner is also asked to: “Provide an estimate of the target’s reaction if the deception is successful. Also provide likely target reactions if the deception is not successful. Identify whether the adversary would use deception in response. This subparagraph provides in-depth information to document the risk assessments presented in Tab C-3-A (Military Deception) and Exhibit C-3-A-3 (Operations)” (HQMC 2001f, G-54).

Since the analysis of an adversaries deception effort is part of the Marine Corps’ doctrine, one could assume that the Marine Corps practices this capability during training and operations. Counterdeception is not a tangible capability but rather the ability of a Marine commander and his staff to make informed decisions about countering the enemies deception effort.

Counterpropaganda Operations

The next element of DIO that will be explored is counterpropaganda. To execute these types of missions, a military force must have a PSYOP capability. The definition of PSYOP is: “Psychological operations are planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately, their behavior. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives” (CJCS 2001, 343). Additionally, counterpropaganda is defined as: “Activities identifying adversary propaganda contribute to situational awareness and serve to expose adversary attempts to influence friendly populations and military forces” (CJCS 1998, III-7). The Marine Corps’ ability to conduct these types of operations is

limited in size and scope. The doctrine for joint PSYOP outlines the Marine Corps PSYOP capabilities. "The USMC has the capability to execute observable actions to convey selected impressions to support PSYOP objectives. This support can include the use of shore-based loudspeaker broadcasting, aerial and artillery leaflet dissemination, combat camera documentation, and use of motion picture projection and viewing equipment" (CJCS 1996, A-2). Since these are the only PSYOP capabilities organic to the Marine Corps, the MAGTF must seek outside support for any sizeable PSYOP effort. MAGTFs will normally be supported with a PSYOP detachment. These detachments will come from the Army's 4th Psychological Operations Group (4th POG) (Tull 2000, 12). The following describes the nature of this support obtained from the 4th POG: "4th POG/Brigade PSYOP Support Element, 4-6 man HQ and 4 man teams, one for each maneuver element . . . During conflict or tension, 4th PSYOP Group provides a staff to refine plans. Stationed at Fort Bragg, NC, it is the only active Army PSYOP unit, and constitutes one-quarter of all US Army PSYOP units; the rest are reservists" (Tull 2000, 12). Army Field Manual (FM) 90-29, Noncombat Evacuation Operations, outlines the capabilities of the 4th POG. These capabilities are:

> Analyze potential targeted audiences to identify critical communicators and media, cultural and language nuances, and applicable themes and symbol. Develop programs and products which support supported CINC's mission and objectives, based on the above analysis. Employ organic and nonorganic assets to develop print photographic, audio, visual, and audiovisual products, which support these programs. During contingency operations, the senior PSYOP headquarters is doctrinally OPCON to the supported CINC, JTF, or combined task force (CTF) commander. In accordance with the Joint Strategic Capabilities Plan (Annex D), 4th POG is charged with providing the Joint PSYOP Headquarters with joint operational level focus and developing the CINC or commander's joint or combined PSYOP campaign plan. This includes integrating other service PSYOP assets into the plan. Maneuver units normally have tactical PSYOP elements attached to execute the face-to-face dissemination. The 4th

> POG is capable of providing PSYOP support ranging from propaganda and product development, to media production, to strategic, operations, and tactical information dissemination. The 4th POG's organic media assets include light-to-heavy print production; audio production; amplitude modulated (AM), FM, and short-wave radio broadcasting stations; audiovisual production and dissemination; and tactical loudspeaker dissemination. (HQDA 1994, A-1)

With support from the 4th POG, the MAGTF can be integrated into the overall campaign PSYOP effort. Another capability that the Marine Corps can request is called COMMANDO SOLO. This capability is described in the MAGTF Staff Training Program (MSTP) brief as: "COMMANDO SOLO C-130s from Pennsylvania Air National Guard (193 Special Operations Wing in Harrisburg, PA, now a reserve mission) . . . capable of conducting PSYOP and EW; capable of color TV broadcasting throughout TV UHF/VHF ranges; high-powered transmitters can jam adversary hard-liners with TV and radio broadcasts or simply overpower signals and replace propaganda with PSYOP programs" (Tull 2000, 12). In addition to the COMMANDO SOLO capabilities, the Air force also has the "MC-130 COMBAT TALON force, based in CONUS, Europe, and the Pacific, is fully trained and equipped for leaflet dropping operations" (CJCS 1996, A-2). MAGTFs may also receive support from PSYOP production facilities. "Production facilities (leaflets, video) will remain at the CINC or Ft. Bragg" (Tull 2000, 12). These facilities produce the PSYOP products to be disseminated to target populations. Based upon the tactical situation and the PYSOPs plan, Marine Corps planners should incorporate the capabilities offered by the 4th POG, COMMANDO SOLO, COMBAT TALON force, production facilities, and their organic capabilities into their plans to ensure the effects of the PSYOP properly support their tactical mission. During crisis situations, adversary forces may have control of the local media outlets and use them to

run their own PSYOP or propaganda campaign. Therefore MAGTF planners must ensure they properly counter the adversary propaganda with their own propaganda. To gain the best advantage, these planners should consider all PSYOP means available.

Electronic Warfare

The last element of DIO that will be reviewed is that of EW. EW is defined as: "Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy" (CJCS 2001, 141). The Joint doctrine continues to define EW in three subdivisions. The three subdivisions are electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA is defined as:

> That division of electronic warfare involving the use of electromagnetic energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability and is considered a form of fires. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). (CJCS 2001, 141)

EP is defined as:

> That division of electronic warfare involving passive and active means taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. (CJCS 2001, 141)

ES is defined as:

> That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition, targeting, planning and conduct of future operations. Thus, electronic warfare support provides information required for decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. ES data

> can be used to produce signals intelligence, provide targeting for electronic or destructive attack, and produce measurement and signature intelligence. (CJCS 2001, 141)

As with the other elements of DIO the Marine Corps has the ability to execute EW missions. The current Marine Corps capabilities to conduct EW are the EA-6B aircraft, and the Radio Battalion. "The Marine Corps EA-6B Prowler provides Airborne Command and Control (C2W) support to Fleet Marine Forces to include electronic attack (EA), tactical electronic support (ES), electronic protection (EP) and high speed anti-radiation missile (HARM)" (FAS 2002, 1). Although the EA-6B is a capable aircraft, it may not be available to the MAGTF when it is needed. "The EA-6B is considered a low density-high demand strategic asset and may not always be available to support MAGTF operations" (Tull 2000, 12). Additionally, the Marine radio battalion is "capable of conducting tactical signals intelligence, COMSEC monitoring and EW" (Tull 2000, 12). The main deployable EW capability in the radio battalion is the Mobile Electronic Warfare Support System team.

> One of the most versatile assets 2nd Radio Bn. brings to the battlefield is the Mobile Electronic Warfare Support System team, a multi-faceted five-man element tasked with providing communications intelligence on the enemy, locating his position, and disrupting his ability to communicate. The team operates out of a hybrid version of the light armored vehicle(LAV). The LAV is equipped with an extensive communications suite that permits the electronic warfare specialists inside to monitor enemy activities. Operations can be carried out whether the unit is stationary with the battalion landing team headquarters, or on the move with the light armored reconnaissance platoon. (Fahy 1997, 1)

This capability coupled with those of the EA-6B provides the MAGTF with a robust EW capability.

In conclusion, the MAGTF has many capabilities to conduct DIO: IA, physical security, CI, OPSEC, counterdeception, counterproagada, and EW. While these

capabilities do exist, the MAGTF will require constant modernization and training to implement a viable DIO plan. Chapter 5 of this thesis will provide examples of how these DIO elements have impacted past operations.

CHAPTER 5

HISTORICAL EXAMPLES OF DIO

Military history provides examples to be studied by military planners. This chapter will use military history to cite examples of how DIO has been used during past military operations. Each element of DIO will be studied: IA, physical security, OPSEC, CI, counterpropaganda, counterdeception and EW. These historical examples will then be used to support the thesis conclusions in determining which elements of DIO should be carried out by the MAGTF. This historical review will provide the reader with a better understanding of the impact that DIO elements have had on past military operations.

IA and the Kosovo Conflict

Many have called the Kosovo conflict the first cyberwar. During this NATO operation, many information systems were used by NATO commands in the execution of the campaign. Since NATO consists of nineteen separate nations and has many headquarters facilities dispersed around Europe, they rely on their information systems to perform command and control functions. This reliance on networks creates a vulnerability that can be exploited by an adversary. During the Kosovo campaign, there were many attacks directed against NATO networks. Although these attacks had minimal operational impact, they did identify vulnerabilities in NATO's network infrastructure. These network attacks also provided NATO planners with the realization that these attacks could emanate from virtually anywhere in the world. Anyone sympathetic to the Serbian cause that had access to an Internet-connected computer could launch an attack.

> During the Kosovo crisis, attacks were reported from sources in Serbia and Russia, as well as from sympathizers in other countries, on NATO systems, US government systems, and defense systems of coalition partners. Apart from denial-of-service attacks and defacing of web sites, attempts were made to intrude defense networks . . . Daily, one can find articles in the news about hacked systems, intrusions in Defense and government systems all over the world and affected infrastructures. However, full scale attacks with a major impact on Armed Forces and/or society have not (yet!!) been realized. (Luiijf 2000, 5)

In this quote, Luiijf ends his thought with the fact that the military has not experienced a large-scale network attack against military operations. Since the attacks on the NATO networks were limited in scope, NATO was able to work around the problems created by these attacks. Luiijf continues to discuss the fact that many different players were involved in these attacks. This fact makes the protection of networks increasingly difficult. Additionally, the diversity of the attacks posed a problem for those defending the NATO networks. These multiple attacks from various means caused NATO to weaken their control and slowed their momentum because information systems were disrupted.

> As an example, Serb hacktivists tried to attack NATO and coalition Defence and government systems during and after the Kosovo crisis. Assist [sic] was given by Russian and later Chinese (State) hackers. Email bombs, viruses, denial-of-service attacks, port scans and intruder tools were used as means to attack these systems. Prepared only for information provision in peacetime, the overloaded NATO systems went to their knees until adequate corrective measures were taken. Note that as a side effect, denial-of-services at NATO and coalition web sites caused people to turn to other sources (e.g. CNN) that published information in a less 'time-controlled' and verified manner. Thus, the accessibility of a public-relations system turned out to be more crucial for the (public support of) operation as ever was understood before. (Luiijf 2000, 3)

In addition to a direct threat from a known adversary, the military learned that other outside threats exist which are not directly targeted at the military but can disrupt military information systems. The Melissa virus of 1999 is an example of a computer worm virus

that affected many military information systems during the Kosovo conflict (Luiijf 2000, 5). This virus, which was the first of its kind, when executed, would cause a denial of service to the victim by overloading the network with spurious email messages. "The virus proceeds to propagate itself by sending an email message in the format described above to the first 50 entries in every Microsoft Outlook MAPI [messaging application programming interface] address book readable by the user executing the macro. Keep in mind that if any of these email addresses are mailing lists, the message will be delivered to everyone on the mailing lists" (Carnegie Mellon University 2002, 1). This virus, while not directly targeted at the NATO operation, did have an impact on the NATO networks resulting in a denial of email service. The lesson learned from the Melissa virus is that network attacks can come from many sources and not just those of an adversary force. Military planners must be prepared for such attacks by continually building and improving network defenses. John Hamre, Deputy Secretary of Defense remarked on the defenses of military networks during the Kosovo crisis:

> The cyber attacks on NATO have been 'very incoherent and amateurish.' He also said the attacks likely were Yugoslav-sponsored but probably not conducted by the Serb-controlled government but messed up the NATO home page. Adding, It's all directly tied to the war. Two years ago we had our first cyber terrorist attack. Called 'Solar Sunrise,' it showed hackers that the nation's weakest link is its electrons and we're seeing that in spades now. Two years ago we didn't have a map of the networks. Now we do. Two years ago we didn't know our Web sites. Now we do. One year ago, we didn't have firewalls. Today we do. A year ago we wouldn't have real-time information on intrusion and detection. Today we do. (Hamre 1999, 1)

This statement demonstrates the fact that military planners realize the need for computer network defenses and are taking active measures to mitigate network attacks even though they have not been attacked with a large-scale coordinated network attack. As a result of

these attacks, the US military has begun educating their personnel on the requirements for network security. The DOD CAC (smart card) program will also strengthen the ability to secure passwords and user authentication. Additionally, the DOD has begun working with the commercial software industry to ensure that security flaws are corrected. The main lesson learned from the Kosovo network attacks is that an attack can originate anywhere and can be designed to defeat known network defenses. With that said, the need to continually improve network defenses must not be overlooked.

Physical Security and the Terrorist Attack

Modern day warfare has taken a different form when compared with the traditional force on force operations of the past. Today military forces and civilians face the threat of terrorist attacks. These attacks can come in any form and likely, when least expected. Since terrorist attacks have become more frequent, the military planner must consider physical security as the first line of defense for a military force. As such, physical security must be integrated into the IO planning to ensure the key command and control (C2) nodes are protected. To date, terrorist actions have focused on targets with weak defenses such as a barracks or a ship pulling into port, but the fact that C2 nodes have not been directly targeted might indicate that the military is properly securing these facilities. That fact that terrorists use asymmetric means to attack their targets means that the IO planner must use past attacks as examples of how C2 centers might be attacked in the future. The protection of these C2 centers must be included in the overall force protection plan. As stated by Secretary of Defense William J. Perry in remarks made after the Kobar towers bombing: "Force Protection is a key component of all mission analyses and must be continually reevaluated and updated as the operational mission

progresses. It must include offensive and defensive measures. . . . Successful physical security and force protection operations rely on the ability to detect and assess threats, to delay or deny the adversary access to his target, to respond appropriately to an attack, and to mitigate the effects of an attack. . . . Modern physical security and force protection technology systems can provide significant enhancements to security in vulnerable locations" (Perry 1997, 1). Additionally, similar to the Khobar towers event were the terrorist attacks on the US Navy ship USS *Cole*, the twin towers of the World Trade Center, and the Pentagon. These events used unconventional means to strike at their targets. "The 11 September 2001 terrorist attacks on the World Trade Center and the Pentagon, and the 2000 attack on the USS Cole are examples of asymmetric or asynchronous acts carried out by an adaptive and thinking opponent who continually studies the strengths and weaknesses of his perceived enemy and adapts his operations accordingly. These attacks were not without a larger purpose. They are part of an ongoing campaign that is likely to continue and expand" (Shaughnessy and Cowan 2001, 5). As the quote states, terrorism is an ever-evolving threat that military planners must be prepared to face. The physical security challenge becomes increasingly difficult to meet since the terrorist threat uses varying methods of attack. Military planners must consider these threats during all phases of a military planning. They must look at the methods of conducting military operations during both peacetime and wartime to identify potential weaknesses in the protection of the force. Military planners must realize that the adversary will strike at the time and place of his choosing and not necessarily at the targets that the military expects them to attack.

"The terrorist picks the time and place of the event rather than having the time and place defined by its relationship to other operations. This represents an offensive framework that is driven by vulnerability, opportunity, and tailored capability rather than by fixed capability employed in a conventional construct. Because these events are asynchronous, it does not mean that they are not part of a larger, more synchronized effort. In fact, it is becoming increasingly more likely that future terrorist tactics will be employed in a more synchronous operational framework" (Shaughnessy and Cowan 2001, 3). The attack on the USS Cole identified the vulnerability of ships as they pull into foreign harbors and rely on host nation support to park pier side. This vulnerability is just one aspect of physical security that should be considered when planning military operations. Since the military relies heavily on contracted labor from many foreign sources, the task of conducting vulnerability assessments becomes vitally important. As a result of the Khobar towers bombing, DOD has adopted a new method of determining the vulnerabilities to US controlled facilities.

> The joint staff integrated vulnerability assessment (JSIVA) teams were formed in 1997 following a DoD task force report on the 1996 terrorist attack on Khobar Towers, Saudi Arabia. The report reviewed the adequacy of security at Khobar Towers and the surrounding area as well as force protection funding, resources and coordination of intelligence and antiterrorism countermeasures on a large scale. The task force found that the DoD had no published standards for force protection of fixed facilities. Their recommendations included: establish prescriptive DoD physical security standards; designate a single DoD agency to develop, issue and inspect compliance with security standards; provide the designated agency with sufficient resources to assist field commanders on a worldwide basis with force protection matters; and provide funds and the authority to the agency to manage research and development efforts to enhance force protection and physical security measures. (DTRA 2000, 1)

From this study, the JSIVA teams were formed. These teams conduct detailed analysis of military facilities to identify vulnerabilities that could be exploited by a terrorist. These

teams also study the regional terrorist organizations in hopes of identifying potential methods of attack and potential targets. The JSIVA is a valuable tool for commanders to evaluate the physical security of their own military facilities. Catastrophic events, such as these terrorist attacks, provide military DIO planners with the best examples of how an adversary can exploit physical security vulnerabilities.

OPSEC in Desert Storm

History has demonstrated the importance OPSEC plays in conducting military operations. Information on enemy plans and locations can provide an operational advantage thus making OPSEC of the utmost importance. Operation Desert Storm demonstrated how good OPSEC provided this advantage. Both the US led coalition and the Iraqi forces used OPSEC to gain an advantage: "By combining OPSEC and deception under unity of command, General H. Norman Schwarzkopf was able to maneuver coalition forces to surprise, shock, and dislocate Iraqi forces. General Schwarzkopf's hint of an amphibious landing drew critical Iraqi forces away from the real coalition plan. When Schwarzkopf topped this deception with an attack at blinding speed, Saddam's battered forces could not react" (CJCS 1997, X). This example demonstrates that the security of operational information is paramount for the success of a deception plan. OPSEC enabled General Schwarzkopf to convince the Iraqi's that he was planning an amphibious invasion of Kuwait which in turn caused the Iraqi's to heavily defend the shoreline of Kuwait. General Schwarzkopf was careful to position units for the actual offensive only when he believed the timing essential. He did not want the deception plan revealed due to leaked information of such force movements. COL Julian A. Sullivan, Jr., Commander of the 507th Support Group during Desert Storm mentions the impact of

OPSEC on his support to the operation: "For any number of reasons, and it primarily had to do with OPSEC and so forth, the CINC, GEN [H. Norman] Schwarzkopf, made a decision that we would not move in to Log Base CHARLIE until the bombing campaign started or until what we call D-Day" (Sullivan 1991, 1-2). This example shows how the concious decision to move the log bases at the last minutes prior to the attack meant that the Iraqi's could not easily locate and attack these facilities. The use of cover and concealment by using EW to blind the Iraqi radars and communications was also an enabling force in reference to OPSEC. During Desert Storm, OPSEC was used by both sides. The Iraqi's used OPSEC to disguise the true status of their fielded forces.

> As the fifth week of the war began this week, senior Pentagon officers made the following points about the progress of the fight: Iraqi 'OPSEC,' or operational security, has been surprisingly effective, in part because of a resilient fiber optic communications line running underground from Baghdad to Basra and on to Kuwait. Allied bombers have struck a number of microwave communications towers, including several in remote villages, but have had difficulty severing the fiber optic cables. As a result, the allies have had limited success in forcing Iraqi commanders 'up into the air'--giving orders by radio--where such communications are vulnerable to US eavesdropping. *(*Atkinson 1991, A01)

This example demonstrates that the Iraqi military understood the threat from the coalition and took active measures to ensure the integrity of their OPSEC. By these OPSEC measures, the Iraqi's were able to disguise the true status of their military forces. These examples highlight the fact that successful OPSEC can be used to counter the threat of adversary CI and lead to greater success on the battlefield.

Counterintelligence in Bosnia

As stated in previous chapters, CI is a vital intelligence function in support of deployed forces. US forces rely on CI teams to paint a clear picture of the enemy threat and offer measures to counter those threats. CI teams are normally deployed as small

units consisting of a two to six man teams. In Bosnia CI teams have provided deployed US commanders with timely and accurate information supplying them with vital situational awareness. The following Bosnia scenario furnish lessons learned that can be applied by Marine Corps CI teams in future operations:

> In an effort to counter the non-traditional threats confronted in this multinational peacekeeping operation, CI and HUMINT elements were called upon to provide, coordinate, deconflict, synchronize, and integrate an unusually wide variety of intelligence support. That support included counterintelligence collection, threat and vulnerability assessments, liaison with local law enforcement and foreign military security and intelligence services, CI Force Protection Source Operations, Technical Surveillance Countermeasures (TSCM), debriefing of US and allied soldiers, debriefing and screening of displaced persons or refugees and detainees, investigations and analysis, exploitation of foreign documents and equipment, and timely dissemination of hand-held digital imagery. (Perkins 1997, 241)

This effort of countering the non-traditional threat requires a high operational tempo due to the ever-changing situation. Within the US sector of Bosnia CI personnel require the authority to operate outside of the normal Army standing operational procedures to enable them to complete their missions.

> The operational tempo for the CI and HUMINT operators both forward-deployed and in support, was extremely high. Initially, tactical teams were restricted in movement due to force protection concerns. Eventually the Task Force commander, understanding the importance of the CI and HUMINT team mission, authorized an exception to policy for CI and HUMINT Teams. He allowed them to travel in two-vehicle convoys, as opposed to the standard four-vehicle convoys, during daylight hours. Travel required a brigade or battalion commander's approval. Travel at night required general officer approval and four vehicles. This made liaison dinners a challenge, but they did get approved. CI and HUMINT operators at the division level and those teams assigned to the Nordic brigade were able to use this important exception to policy. US brigade commanders, however, were not required to implement this policy and therefore continued to require their teams to travel in four-vehicle convoys. This did not deter the teams. They became experts at organizing a four-vehicle convoy of military police, civil affairs, or whatever kind of personnel they could find heading out of the base camp. (Perkins 1997, 241-242)

Because these actions happened in recent years, the lessons learned are relevant to near term future operations. CI operators were able to demonstrate their importance to the operation by performing the above missions. Since the mission in Bosnia is a peace enforcement operation with the NATO-led coalition standing between former warring factions (FWF), military CI operations were critical. Additionally, the race to provide accurate information to both military commanders and the press was required to ensure an accurate understanding of events within Bosnia. CI teams in Bosnia are tasked to scope the press to ensure accuracy of reporting. The incident at the Usora bridge highlights the importance of CI in Bosnia and provides insight into the activities conducted by US CI teams.

> Bosnia was, and still is, an environment where CI and HUMINT operators could show their value added. The threats were real and the PIRs [priority intelligence requirements] were critical to the commander . . . It was an environment of terrorists, criminals, and elements of the three FWFs, all of whom were hard to identify but were well-armed and had significant intelligence collection capabilities including HUMINT. To describe this as a complex and challenging environment is an understatement . . . The Usora bridge incident in early August 1996 is an example of timely, accurate, and high-quality reporting that was collected and processed faster by CI and HUMINT teams than the CNN. A smaller bridge built by the United Nations near the Usora Bridge was badly damaged after a charge had been thrown from a moving vehicle onto it. A tactical CI and HUMINT team immediately responded to the incident and arrived at the scene, interviewed witnesses, took digital photographs of the damage and, within one hour, passed the brigade and the TF commander accurate information. The national intelligence community had the final Intelligence Information Report (IIR) with digital photographs within 4 hours, with most of that time having been taken for imagery annotation. Hence, the standard for CI and HUMINT teams was to beat CNN and tell the real story. (Perkins 1997, 242)

CI teams effectively countered a threat from an adversary who attempted to use a media event to send a false impression of a situation. In many cases, CI teams got to the scene and assessed the situation prior to the press, they released accurate information to the

press thus ensuring accurate reporting of events. Also, since the teams were able to rapidly relay the facts about the bridge bombing back to the task force commanders, the commanders had more time to use the information in their decision making process. Marine DIO planners should study the CI examples from Bosnia to learn how CI can be integrated into the overall DIO plan.

Counterpropaganda in Somalia

Propaganda can play a significant role in military operations. Military planners should realize the potential effect propaganda has on military operations and make plans to counter adversary propaganda messages. During the United Nations Operations, Somalia II (UNOSOM II) peace enforcement operation, propaganda was used by both the UN forces and Somali warlords to support their operations. The leader of the Somali warlords was Mohammed Aideed. Due to his status within Somalia, Aideed became the target of UN military operations. The goal of the UN propaganda campaign was to counter Aideed's messages and minimize his influence within Somalia.

"The first solid step toward personalizing the conflict and 'marginalizing' him was the attack on Aideed's radio station. Although the station had been spewing forth a steady torrent of anti-American and anti-UN propaganda, it had been successfully countered through a US counterpropaganda campaign. Seeing a peaceful approach as more credible, UNITAF and Ambassador Oakly took the stand that it was Aideed's right to broadcast whatever he wished. The US simply fought him with the truth on their own radio station. Their highly successful approach included positive stories using extensive interviews with local Somalis to counter Aideed's lies, often using members of Aideed's own clan to refute him" (Bullock 1995, 44-45). This use of counterpropaganda enabled

the UN forces to build credibility by using truth as a means to destroy the credibility of Aideed and his forces. Additionally, using Aideed's own people to send some of the messages enabled the UN forces to gain insider information about Aideed to use against him. Since propaganda is reliant upon credibility, the use of these former Aideed clan members enabled the UN messages to hit directly at what was uniquely important to the Somali people.

Although this example of counter propaganda was somewhat successful, the UN mission still ended in failure. Because of this, military planners should understand that counterpropaganda is only one aspect of DIO, within a military operation. It must be integrated with other military capabilities to ensure the greatest chance of mission success. In this Somalia example, mistakes were made at the highest levels of UN command, which had a drastic effect on the UN propaganda campaign.

> UN Secretary General Boutros-Ghali continued to make sweeping statements about completely disarming the country. This move threatened every warlord but put special stress on Aideed because of his already high visibility in Mogadishu. Another factor accelerating the rush to open war was the loss of corporate knowledge and experience after the change of command to UNOSOM II and from Ambassador Oakly to Admiral Howe . . . Our attempt to impose a total solution required a clear enemy. When faced with an abstract enemy like lawlessness or brutality, Americans tend to take sides or create a visible enemy. While UNITAF could afford to remain distant, UNOSOM II's ambitious mandate made this approach much more difficult . . . Our desire to impose a US/UN solution based on Jeffersonian democracy led UNOSOM II to be too ambitious and dictatorial in its 'solution.' While in Somalia and believing that 'half a glass may be the best we can hope for,' our focus on ideal democracy pushed us to reject an unsatisfying Somali solution and ultimately led to failure. In hindsight, almost everyone sees singling out Aideed as our enemy to be an overall liability. In the words of end-state planning authority, Col Bruce Clarke, 'Even in chapter 7 ops, . . . you must maintain neutrality if you are to avoid becoming involved on the side of a given faction and remain effective.' (Bullock 1995, 45)

This quote demonstrates a failure to understand the culture and identify an achievable endstate in the overall UN counterpropaganda campaign. The counterpropaganda effort must be understood at all levels of military operations because all messages broadcast to the press can impact public sentiment towards the military operation. In this example the UN Secretary General made the mistake of giving the impression that all Somali's would be disarmed. This message within Somalia did not receive a positive reaction. Somalia is a warrior culture and the Secretary General's message only inspired the warlords to take more direct military action against the UN forces. This UN message helped lead to the ultimate failure of the UN operation. Propaganda must be understood by all levels of the military command structure and must be carefully planned to ensure the wrong message isn't sent which could damage the ultimate goal of the military operation. In Somalia, the tactical level counterpropaganda campaign was working, but messages from the strategic level had a damaging effect on the operation.

Counterdeception in Desert Storm

Deception is another aspect of military operations that can aid in the success of military operations if properly employed. During Operation Desert Storm, the US-led coalition used deception to counter the Iraqi forces that were dug into defensive positions along the Persian Gulf coastline in Kuwait. The Iraqi's used deception along the boarder of Kuwait and Saudi Arabia where they created an obstacle belt with mock tanks and other fake military equipment incorporated into these defenses. Countering this Iraqi deception, the US developed its own deception plan using an afloat MAGTF. Many international press articles were written depicting the invasion of Kuwait with a US Marine Amphibious landing. This threat to the Iraqi military forced the Iraqi's to

position forces to defend the coastline of Kuwait. While the Iraqi's were defending the coast, the coalition forces did not really intend to conduct an amphibious landing thus deceiving the Iraqis and splitting their forces. The below quote is an example of how the international press supported the credibility of the deception operation:

> It has been taken for granted in the Soviet press that US forces would conduct amphibious operations against Iraqi forces. . . . Lieutenant General Skuratov discussed the nature of an American amphibious landing in the Persian Gulf. 'Taking into account the presence of a large contingent of US Marines and amphibious forces in the region,' he observed, 'one can presume that they will conduct amphibious landings . . .' Skuratov analyzed American and British amphibious landings during the Korean, Middle East, and the Vietnam Wars, and the Falklands Conflict. He emphasized the growing role of helicopters and hovercraft in US Marine amphibious landings. Shuratov calculated that a force of 2000 to 2500 Marines (two-three battalions) supported by a tank regiment, two-three artillery batteries, one-two antiaircraft batteries, additional armored equipment and armored tank and engineer platoons or companies could be landed in one hour. He went on to compute that an independent Marine brigade, along with a minimum amount of equipment, could be landed in three hours; with all combat equipment - in up to half a day. Skuratov pointed out that onshore Marine operations were characterized by high maneuverability, with some LAV units operating in enemy territory, more than 200 kilometers from the beachhead. Skuratov's article is indicative of the success of the allied disinformation campaign in the Persian Gulf. The inevitability of a Marine amphibious assault into Kuwait received world-wide press coverage. American amphibious exercises and the subsequent threat of a landing by US Marines kept a significant Iraqi force close to the shores of the Persian Gulf, while allied forces executed a strategic envelopment. It is high praise for the allied plan that in the end, even the Soviets, long considered the masters of deception, were themselves deceived. (Villahermosa 2001, 6-7)

This example demonstrates how counterdeception was used to against the Iraqi deception effort. This counterdeception resulted in many Iraqi units being stationed along the border of Saudi Arabia. This counterdeception plan was used to have a decisive effect on the overall military operation. Since there are many examples of how deception and counterdeception have been used to support military operations, counterdeception plans should always consider potential enemy plans and how to defeat them. For a

counterdeception plan to work, it must be credible and the intent of the deception must be guarded. As in the above example, the deception plan highlighted the capabilities of the Marine amphibious forces, which was a credible force with a real capability to conduct offensive operations. Since this was a credible threat, the deception worked. This example also demonstrates the need for secrecy to ensure a counterdeception plan is not revealed. Counterintelligence, and the use of propaganda, can support a counterdeception plan. When properly executed, the right message is put forth to plant the idea of the deception into the minds of the enemy forces. US military forces can guide the press to cover specific aspects of their military capabilities, this will highlight those capabilities needed to support the counterdeception. As demonstrated in this example, counterdeception is a necessary part of military operational planning and should always be integrated with the other elements of DIO.

Electronic Warfare in the Kosovo Conflict

The Kosovo conflict highlighted a need for EW capabilities. During the Allied Force air campaign, EW played a key role in supporting DIO into Kosovo. During this operation, the primary means of EW was the use of EA-6B aircraft. “Gen. Wesley Clark, the operation's military leader, described how critical a role EW played in the allies' success. He testified that ‘we couldn't have fought this war successfully without the EA-6B contribution. We really need the Electronic Warfare capacity that we have there’ ” (Bolkcom 2001, 59). During this operation EA-6B aircraft were extensively used against the Serb defenses. Additionally, these aircraft were employed in a DIO role which provided electronic protection to other Allied aircraft flying in the operation. As a result of this operation, the US military realized the importance of correcting shortfalls in EW

assets. Because of this shortfall, soon after the conflict, the US military leadership pushed for more funding to provide additional EW assets to the US military. "To address one of the most pressing concerns to come out of the war in Kosovo, the Pentagon has appropriated $389 million to accelerate improvements to the EA-6B electronic warfare aircraft and to add a fifth expeditionary squadron of the planes to the inventory. The EA-6Bs were stretched thin during the war to conduct electronic warfare attacks against Serb air defense systems, enabling 38,000 attack sorties to be carried out with no casualties" (Verton 2000, 1). The fact that allied air forces had no casualties demonstrate how EW provided the proper protective measures to these forces. Allied force planners used the EA-6B extensively during the Kosovo operation, which highlighted the need for this capability in both offensive and defensive roles. The EA-6B, when integrated with other joint EW assets, can provide complete EW coverage and high degree of electronic protection. "Although Allied Force was considered by many to be a small scale contingency, 'US systems such as RC-135 Rivet Joint electronic intelligence aircraft and EA-6B tactical airborne Electronic Warfare aircraft were employed in numbers roughly equivalent to those anticipated for a major theater war, and even then were heavily tasked' " (Bolkcom 2001, 60). These EW assets provided DIO by supporting protection to the air campaign. This example demonstrates how these assets when available can be tasked to provide DIO during military operations. A vital portion of the air campaign is the ability to disrupt enemy air defenses and protect friendly forces. The fact that the US military is spending money to add additional EW assets to their arsenal also confirms the need for this important capability. Many articles written after the Kosovo conflict highlighted the importance of EW and the fact that the US has a need for more EW

assets. The effects of EW must be understood by the DIO planner to ensure these capabilities support the overall DIO plan.

This chapter has confirmed the need for DIO in military operations by analyzing past military experiences. Although these examples are brief and limited in scope, they are used to illustrate how each element of DIO has been used and could possibly be used in the future. Each example used recent operations to demonstrate how the elements of DIO were executed with modern military and worldwide informational capabilities. These illustrations also demonstrate that each element of DIO should be used together as an integrated defensive approach to IO. This chapter will be used to draw conclusions on how MAGTF forces can employ DIO in support of future military operations.

CHAPTER 6

CONCLUSIONS AND RECOMMENDATIONS

The purpose of this thesis is to determine what doctrinal principles will enable the MAGTF to conduct DIO. Each element of DIO was examined to determine how it could be integrated into operational planning. This chapter will draw some conclusions on each of these DIO elements and make recommendations on how to incorporate each into MAGTF planning. Additionally, this chapter will offer answers to the primary and secondary questions posed in chapter 1, discuss the significance of this thesis and its relationship to previous studies, suggest areas of further study and provide a thesis summary.

Information Assurance Conclusions

This thesis identified the need for IA to support military operations. Using the historical example of how IA tools were effectively used during the Kosovo campaign, one can conclude that the protection of military information systems is key to conducting modern day military operations. Although this example was not Marine Corps specific, it did furnish the basic foundation of what IA can provide the MAGTF. IA, being a defensive capability, should deny adversaries attempts to disrupt, destroy, and deny friendly information systems and protect these systems from an adversarial attack. Since military networks continue to grow in size and complexity, the need for a continuous defense of these networks becomes increasingly important. The MAGTF must ensure that they incorporate the latest IA technologies to provide for the desired level of protection. As the Kosovo example demonstrates, many factors can interrupt military

communications capabilities and therefore, the MAGTF planner must be aware of these threats and build their network defenses to defeat them.

IA Recommendations

Nine recommendations are provided in regard to the topic of IA and the MAGTF.

1. That the MAGTF incorporate network defenses (firewalls, intrusion detection, encryption, and PKI) into all fielded information systems to ensure that vulnerabilities are minimized.
2. That the MAGTF establish strict guidelines for the use of information systems, especially those unclassified systems that are connected to the Internet since these systems are vulnerable to attacks originating from anywhere in the world.
3. That the MAGTF understands IA policies of each geographic CINC. This will ensure that regardless of where in the world the MAGTF deploys, they will understand the IA policies and be prepared to comply with them. The MAGTF G6 should communicate with the CINC's to ensure they understand the policies prior to deployment of the MAGTF.
4. That the Chief Information Officer (CIO) of the Marine Corps consolidate all theater IA policies and publish them for use by MAGTFs.
5. That the MAGTF report any newly identified vulnerabilities up their chain of command to the CIO of the Marine Corps, to ensure that gaps in their network defenses are understood and that someone is identified to determine countermeasures for these new vulnerabilities.

6. That the MAGTF incorporate IA attacks into their pre-deployment training to ensure that their Marines are prepared to take the appropriate actions when receiving such an attack. These IA attacks should be incorporated into all MAGTF exercises.
7. That the MAGTF communication officer (G6/S6) be responsible for IA. The G6/S6 will report to the MAGTF operations officer as a member of an IO planning cell.
8. That JP 3-13 definition for IA be adopted as the Marine Corps definition and used to guide the development of Marine Corps IO doctrine.
9. That these aforementioned recommendations be incorporated into Marine Corps IO doctrine to ensure a basic understanding of IA throughout the entire Marine Corps.

Physical Security Conclusions

This thesis demonstrated how physical security is a fundamental element of DIO. The historical examples focused on the terrorist attack because terrorism appears to be the largest threat to military operations in the current operating environment. The recent attacks on military forces by terrorists have created a renewed focus on physical security across the US armed forces. The fact that the September 11th attack on the Pentagon was aimed at hitting the military leadership demonstrates that terrorists are targeting the US military leadership. Understanding that an attack (the "threat" is always there) can come at any time and virtually anywhere, the need for tighter physical security measures must be well understood by all military personnel. MAGTF planners must continually attempt to identify the vulnerabilities of their forces and take physical measures to ensure those

vulnerabilities are minimized. The MAGTF should be well equipped to take such security measures since physical security is one of the basic tasks that all Marines perform during their military service. However, the MAGTF must incorporate these security measures into all aspects of their training and service and ensure that physical security is not taken for granted. Physical security should be a way life for all Marines.

Physical Security Recommendations

Seven physical security recommendations are provided.

1. That physical security planning be incorporated into all MAGTF DIO planning. This planning should be conducted regardless of whether the plan is for an exercise or real world operation.
2. That physical security personnel should be identified for each of the MAGTF commands.
3. That the physical security personnel within the MAGTF should perform physical security drills to ensure they are properly trained to respond to an enemy attack.
4. That MAGTF planners identify and understand the terrorist threat in those areas of the world that they are most likely to be deployed. This task will require MAGTF intelligence personnel to remain current with global threat warnings to ensure that they are prepared to brief the MAGTF staff on the threat situation.
5. That the MAGTF G3/S3 be responsible for planning the MAGTF physical security portion of DIO.

6. That the JP 3-13 definition for physical security be adopted by the Marine Corps and used to guide the development of Marine Corps IO doctrine.
7. That the Marine Corps' IO doctrine include physical security as one of the basic elements of DIO. This will ensure that Marines understand that physical security is not only vital for force protection, but is also required in the protection of military information.

Operations Security Conclusions

OPSEC is another element of DIO that is vital to the successful execution of military operations. The term OPSEC is one that is familiar to most every Marine. One reason this term is so familiar, is because it is the one area of security that is most commonly violated without regard to consequences. Most Marines understand the importance of OPSEC, but because of today's instant and ready access to global communication networks, the tendency to inform loved ones of the military members situation creates a conflict of interest for the individual Marine. The individual Marine might rationalize, that the chances of being targeted by foreign intelligence is small and therefore the chances of leaking vital military information is also very small. This perception creates a large OPSEC vulnerability and requires continual training and reinforcement to ensure all Marines fully understand the importance of OPSEC. Good OPSEC is essential to the success of any military operation and is especially vital during a military deception effort. As with the Desert Storm example, OPSEC enabled the US military to position themselves in a manner that the Iraqi military didn't expect, and therefore, was a key factor in the success of the overall operation. One method used in the success of the OPSEC effort was that most of the fielded forces were limited in their

ability to communicate with family and friends. This decreased the likelihood that information as unit locations and activities would be leaked. For OPSEC to be effective, it must be understood and practiced by all members of the command. MAGTF commanders must continue to reinforce the need for OPSEC and clearly state what type of information is acceptable and can be provided to others outside of the MAGTF. This constant reinforcement will hopefully curb the individual Marine's desire to inform their loved ones, which in turn could leak operational information providing an advantage to the enemy.

OPSEC Recommendations

Seven recommendations are offered in regard to OPSEC:

1. That the MAGTF commander should clearly state his policy on OPSEC to his Marines. This policy should continually be reinforced to ensure that all members of the MAGTF understand it and will attempt to comply.
2. That the MAGTF operations officer (G3/S3) be responsible for OPSEC training.
3. That the MAGTF should always practice OPSEC during training and employ CI Marines and outside agencies to monitor such training. For example the MAGTF could request a Communication Security (COMSEC) monitoring team to assist the MAGTF by monitoring telephone calls and unclassified email for operational information. These COMSEC monitoring teams can provide quick feedback to the MAGTF commander on how well their OPSEC is working. Additionally, the MAGTF can use CI Marines to check the MAGTF's trash for operational information from discarded documents. This

will also provide the MAGTF commander with a better view of how his Marines are taking measures to protect operational information.

4. That the MAGTF employ their own call monitoring of tactical phone networks and employ email filters to ensure secret information is not leaked.
5. That MAGTF commander's must ensure that their subordinates are provided and comply with the OPSEC guidance from higher headquarters and understand the guidance that the geographic CINC's have published for their theaters of operation.
6. That the JP 3-13 definition for OPSEC be adopted by the Marine Corps and used to guide the development of Marine Corps IO doctrine.
7. That the Marine Corps should incorporate OPSEC into their DIO doctrine to ensure all Marines understand the effects OPSEC has on the protection of military information.

Counterintelligence Conclusions

CI is another necessary element of DIO. CI is needed to counter the espionage threat and provide the commander with a planning and assessment capability for countering potential enemy intelligence threats. CI personnel can provide the MAGTF commander with the HUMINT needed to determine if MAGTF OPSEC is effective and to gather a picture of the situation as seen through human eyes. The historical example of the CI teams employed in Bosnia, highlights the fact that CI is multifaceted and therefore can perform a variety of missions dependent upon the commander's needs. CI must be incorporated into all operational planning efforts to ensure that the MAGTF commander has a means of gathering the vital intelligence needed to execute the mission. MAGTF

CI personnel should work with national level intelligence agencies to gain a better understanding of the enemy intelligence capabilities around the world. Since the MAGTF has a limited number of CI personnel, the link into national level intelligence is vital. An added benefit is that the national level intelligence agencies already have an established means of collecting intelligence in most of the hot spots around the world. During operational planning, MAGTF CI personnel simply need to communicate their needs to these national intelligence agencies in order to gain the required situational awareness prior to making any assessments themselves. CI is a vital DIO function that must be continually planned for and executed during all military operations and training events.

CI Recommendations

Seven recommendations are offered in regard to CI:

1. That the MAGTF intelligence Officer (G2/S2) be responsible for CI planning and provide CI expertise to a G3/S3 led IO planning cell.
2. That MAGTF commanders employ their CI teams to support their intelligence collection efforts.
3. That MAGTF CI teams remain abreast of the world situation and stay connected to national level intelligence agencies for current threat information from potential hot spots, which could require MAGTF involvement.
4. That MAGTF CI personnel assist the MAGTF commander in developing his OPSEC policy so that the threat is clearly understood by all.

5. That MAGTF CI personnel understand what military and national level CI capabilities exist within a CINC's theater of operations and be able to request the use of those capabilities required.
6. That the JP 3-13 definition of CI be adopted by the Marine Corps and used to guide the development of Marine Corps IO doctrine.
7. The Marine Corps should incorporate CI into their IO doctrine.

Counterpropaganda Conclusions

In today's era of worldwide mass media, the need for counterpropaganda becomes a key to executing military operations. Counterpropaganda is required to minimize or negate the effects of an adversary's PSYOP effort. In many cases, the adversary may have control of the local print, television and radio media within a specific area. Therefore, MAGTF commanders should understand that countering the effects of these media capabilities could be extremely difficult. MAGTF planners must ensure that they understand their adversary's messages and develop counter messages that attack the legitimacy of those messages. MAGTFs must be prepared to request the use of theater PSYOP capabilities for integration into their operations and should train with those capabilities when possible. Additionally, since MAGTFs do not possess PSYOP trained Marines, they should rely on the expertise of the 4th POG to support their operations. The MAGTF only has loud speakers and the ability to deploy leaflet bombs from their organic aircraft should that be required. MAGTF commanders should ensure that these PSYOP capabilities are fully integrated into the overall operations plan and that any required PSYOP support is requested from the Army's 4th POG. If the MAGTF message is the truth, then public affairs Marines can be used to get the messages into the

media. Propaganda can turn the tide of public opinion and therefore should be considered throughout all phases of a military operation.

Counterpropaganda Recommendations

Five recommendations are offered in regards to Counterpropaganda:

1. That counterpropaganda planning be the responsibility of the MAGTF G3/S3 and incorporated into all MAGTF operational plans. The G3/S3 will require augmentation from the 4th POG to ensure proper PSYOP expertise is found on the MAGTF staff.
2. That the MAGTFs should request PSYOP support during operations and exercises.
3. That the MAGTFs should understand and identify PSYOP capabilities that are resident in each CINC's theater of operations.
4. That the JP 3-13 definition for counterpropaganda be adopted by the Marine Corps and used to guide the development of Marine corps IO doctrine.
5. That counterpropaganda as a element of DIO should be incorporated into Marine Corps IO doctrine.

Counterdeception Conclusions

Deception in warfare can be the difference between success and failure in combat. The ability to deceive an adversary and make them react to this deception, can enable friendly forces to position themselves to achieve success on the battlefield. A good example of how deception can be decisive in combat operations was sited in chapter 5 with the US deception plan in Desert Storm. Had the Iraqi's understood that the Marines afloat were not the actual assault forces, they could have repositioned their forces to

better defend against the inland threat. Since this deception was so successful, the US military achieved an overwhelming victory. This type of deception planning should be done for all combat operations. MAGTF's must ensure that during the operational planning process they attempt to predict the enemy deception plans and develop their own counterdeception plans to defeat the enemy. These plans must be designed to counter adversary deception efforts. MAGTFs should use all the intelligence assets available to determine adversary deception efforts, which in turn will enable the MAGTF planners to develop counterdeception plans. Counterdeception, as with many other facets of military operations, relies on good OPSEC and intelligence gathering capabilities. The deception effort must be integrated with all other elements of DIO to ensure the best chance of success.

Counterdeception Recommendations

Five recommendations are offered in regards to counterpropaganda:

1. That the MAGTF G2/S2 be responsible for counterdeception planning and that they will provide expertise to the G3/S3 led IO planning cell.
2. That MAGTFs ensure that counterdeception plans are closely guarded to make certain that OPSEC failures do not impact the deception effort.
3. That MAGTFs focus intelligence capabilities on adversary deception efforts to support the MAGTF counterdeception plan.
4. That the JP 3-13 definition of counterdeception be adopted by the Marine Corps and used to guide the development of Marine Corps IO doctrine.

5. That counterdeception be incorporated into Marine Corps IO doctrine to ensure that Marines understand the importance of the counterdeception effort within the overall DIO strategy.

Electronic Warfare Conclusions

The ability to disrupt enemy radar and communication systems is vital to the protection of US forces in combat. EW provides this protection by disrupting adversary systems while enabling US systems to operate freely within the combat zone. Although Marine Corps EW capabilities are limited, they do offer the MAGTF a substantial degree of protection from enemy early warning systems. MAGTF planners should incorporate EW into their operation plans. Since the Marine Corps' EA-6B EW aircraft play such a vital role during combat operations, they may be tasked to support other theater level efforts and not just those of the MAGTF. MAGTFs must also use their radio battalions for monitoring and jamming enemy communications. MAGTF planners must ensure that commanders at the highest levels understand the MAGTFs EW shortfalls and should request assets to fill in the gaps. In this day of electronic systems, EW can play a decisive role in military operations.

EW Recommendations

Three recommendations are offered in regards to EW:

1. That the MAGTF G3/S3 be responsible for EW planning and that they identify MAGTF EW requirements and request assets to meet those requirements.
2. That the JP 3-13 definition for EW be adopted by the Marine Corps and used to guide the development of Marine Corps IO doctrine.

3. That EW be incorporated into Marine Corps IO doctrine as both an element of OIO and DIO.

Defensive Information Operations Recommendations

As a result of this research the following recommendations are provided.

1. That the MAGTF G3/S3 be given the overall responsibility for IO planning to include OIO and DIO.
2. That the MAGTF staff provide expertise in their respective occupational fields to the G3/S3 for IO planning.
3. That the Marine Corps use JP 3-13 to guide the development of Marine Corps IO doctrine.

Answers to Primary and Secondary Questions

The primary question this research thesis attempted to answer was "What are the doctrinal principles that will enable the MAGTF to conduct Defensive Information Operations?" Answers to this question were sought by researching joint and service doctrine and by studying many published works on the subject. The doctrinal principles that are outlined in the Joint doctrine for IO are all applicable to the Marine Corps. These principles are in agreement with those outlined in the Marine Corps concept paper for IO. This research has determined that MAGTFs should conduct the following elements of DIO: IA, physical security, OPSEC, CI, counterpropaganda, counterdeception, and EW. Additionally, this research has identified that MAGTFs are very limited in their ability to conduct CI, counterpropaganda/PSYOP, and EW. Marine Corps IO doctrine should highlight these deficiencies and suggest remedies as to how MAGTF planners can request additional assets to fill these deficiencies. After a review of the IO threat, this thesis

outlined the Marine Corps capabilities to counter those threats. Additionally, recent historical examples we used to demonstrate how each of the aforementioned DIO elements have been employed to support military operations. This review demonstrated the importance of DIO to MAGTF operations and supports the recommendations made in this thesis. Throughout this thesis, six secondary questions were also answered. Answers to these secondary questions were designed to provide the reader with a better understanding of IO and DIO in relation to MAGTF operations.

Significance of Thesis

This thesis was written because of the lack of Marine Corps doctrine on IO. This thesis focused on the MAGTF and DIO. It was written to be complimentary to a previous thesis written on the MAGTF and offensive IO. The fact that IO is an integral part of current military operations makes this study significant. The purpose of this study is to provide developers of Marine Corps doctrine with an understanding of DIO in regard to MAGTF operations. The Marine Corps' Doctrine Division recommended this study and a copy of the final thesis will be forwarded to them for their consideration.

Relationship of this Thesis to Previous Studies

As previously stated, this study was written to compliment an earlier study focused on the MAGTF and the offensive elements of IO. This thesis attempted to demonstrate the elements of DIO as outlined in the Marine Corps IO concept paper, and how MAGTF forces can employ those elements.

Suggested Areas for Further Research

Since there is currently no Marine Corps doctrine for IO, there are still many areas in need of further research. The scope of this thesis only provided an overview of

DIO. Each specific element of DIO should be further studied to provide greater detail and a better understanding of how the Marine Corps can incorporate them into their training and operations.

Thesis Summary

In summary, this thesis was written to provide MAGTF personnel with a greater level of IO and DIO understanding. MAGTF forces will use these capabilities in future operations and therefore need to understand the power each element of DIO provides to the defense of their forces. Since the field of IO is still fairly new and not well understood by many Marine planners, this thesis was written to raise the awareness level of this important aspect of military operations. As new hot spots erupt around the globe, MAGTF planners will need to use all tools available to protect their forces. Also, since the threat to friendly military forces seems to be moving from the conventional military enemy to a more asymmetric enemy force, the need for improved defenses cannot be overstated. DIO is just one part of the overall defense of the MAGTF, and each element of DIO is important and mutually supportive in the protection of the MAGTF.

REFERENCES

Adams, James. 2001. *Virtual Defense – The Weakness Of A Superpower,* Palm Coast, FL: Foreign Affairs Magazine, May/June 2001, vol. 80, issue 3.

Aiken, Scott. 2000. *Marine Air-Ground Task Force Offensive Information Operations, Supporting Operational Maneuver from the Sea.* Ft Leavenworth, KS: MMAS Thesis, Command and General Staff College.

Alberts, David S., John J. Garstka, and Fredrick P. Stein. 1999. *Network Centric Warfare: Developing and Leveraging Information Superiority.* Washington, DC: CCRP Publication Series.

Arquilla, John and David Ronfeldt. 1996. *The Advent of Netwar*. Santa Monica, CA: RAND.

Atkinson, Rick. 1991. *Iraqis Called Vulnerable to Land Attack.* Washington, DC: Washington Post. Available from http://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/archive/ post021491_2.htm. Internet. Accessed on 03 May 2002.

Bolkcom, Christopher. 2001. *Electronic Warfare is Dragging.* Arlington, VA: Air Force Association, Air Force Magazine, April 2001 ed. Available from http://www.afa.org/magazine/April2001/0401ew.pdf. . Internet. Accessed on 28 April 2002.

Bullock, Harold E. 1995. *Peace by Committee: Command and Control Issues in Multinational Peace Enforcement Operations*. Maxwell Air force Base, AL: Air University Press web page. Available from http://research.maxwell.af.mil/papers/special_collection/saas/bullock.pdf. Internet. Accessed on 28 April 2002.

Bunker, Robert. 1998. *Information Operations and the Conduct of Land Warfare*. Arlington, VA: The Institute of Land Warfare.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden. 1996. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: AFCEA International Press.

Carnegie Mellon University. 1999. CERT [computer emergency response team] Advisory CA-1999-04, *Melissa Macro Virus.* Pittsburgh, PA: Carnegie Mellon University, CERT advisories web page. Available from http://www.cert.org/advisories/CA-1999-04.html. Internet. Accessed on 28 April 2002.

Chairman of the Joint Chiefs of Staff (CJCS). 1996. Joint Publication (JP) 3-53, Doctrine *for Joint Psychological Operations.* Washington DC: Government Printing Office.

_____. 1997. *Joint Military Operations Historical Collection*. Washington DC: Government Printing Office posted on the Defense Technical Information Center (DTIC) web page. Available from http://www.dtic.mil/doctrine/jel/history/ hist.pdf. Internet Accessed on 28 April 2002.

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

_____. 2000. Joint Publication (JP) 2-0, *Doctrine for Intelligence Support to Joint Operations*. Washington DC: Government Printing Office posted on the DTIC web page. Available from http://www.dtic.mil/doctrine/jel/ new_pubs/jp2_0.pdf. Internet. Accessed on 28 April 2002.

_____. 2001. Joint Publication (JP) 1-02, *Definition of Terms.* Washington DC: Government Printing Office posted on the DTIC web page. Available from http://www.dtic.mil/doctri ne/jel/ new_pubs/jp1_02.pdf). Internet. Accessed on 28 April 2002.

Cordesman, Anthony H. 2001. *The Changing Face of Terrorism and Technology, and the Challenge of Asymmetric Warfare.*Washington, DC: testimony to the Senate Judiciary Subcommitte on technology, terrorism, and government, Center for Strategic and International Studies, CSIS on the Hill web page. Available from http://www.csis.org/hill/ts010327cordesman.htm. Internet. Accessed on 28 April 2002.

Defense Information Systems Agency (DISA). 2001. *Department of Defense Public Key Infrastructure.* Fort Huachuca, AZ: DISA, Joint Interoperability Test Command (JITC) PKI Home, web page. Available from http://jitc.fhu. disa.mil/pki/. Internet. Accessed on 28 April 2002.

Defense Threat Reduction Agency (DTRA). 2000. *Joint Staff Integrated Vulnerability Assessments (JSIVA).* Washington, DC: DTRA Corporate Communication, Fact Sheet, web page. Available from http://www.dtra.mil/ news/fact/ nw_jsiva.html. . Internet. Accessed on 28 April 2002.

Department of Defense (DOD) Access Card Office. 2001. *Department of Defense Common Access Card (CAC) Fact Sheet.* Arlington, VA: DOD Access Card Office, Defense Manpower Data Center web page. Smart Card Basics. Available from http://www.dmdc.osd.mil/smartcard/owa/security.basics?p_SID= THJCRSBJEOR. Internet. Accessed on 28 April 2002.

Fahy, Nat. 1997. *A New Tool for Getting Good Dirt*. Washington, DC: Marines Online, Official Magazine of the Marine Corps, USMC web page. Available from http://www.usmc.mil/marines.nsf/9eb11b0ca47d01f7852562d00 078319f/cb26d043101c3aea85256434006002d9?OpenDocument. Internet. Accessed on 28 April 2002.

Federation of American Scientists (FAS). 2000. *EA-6B Prowler*. Washington, DC: FAS web page. Available from http://www.fas.org/irp/program/ collect/ea-6b_prowler.htm. Internet. Accessed on 28 April 2002

Fogleman, Ronald R. 1995. *Information Operations: The Fifth Dimension of Warfare*. Washington, DC. Defenselink, US DOD Speech, vol. 10, num. 47. Available from http://www.defenselink.mil/speeches/ 1995/di1047.html. Internet. Accessed on 28 April 2002.

Gagne, Cathleen, ed.. 2001. SearchSecurity.Com, definition of *Authentication* and *Nonrepudiation*. Needham, MA: TechTarget, Inc. Available from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html and http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci761640,00.html. Internet. Accessed on 28 April 2002.

Godson, Roy. 1980. *Intelligence Requirements for the 1980's: Counterintelligence*. Washington, DC: National Strategy Information Center, Inc.

Goldstein, Frank L. 1996. *Psychological Operations Principles and Case Studies*. Air Maxwell Air force Base, AL: University Press.

Guisnel, Jean. 1997. *Cyberwars: Espionage on the Internet*. New York, NY: Plenum Press.

Headquarters Air Force Doctrine Center (HQ AFDC). 1998. Air Force Doctrine Document (AFDD) 2-5, *Information Operations*. Washington, DC: HQ AFDC, College of Aerospace Doctrine, Research and Education (CADRE) web page. Available from http://www.cadre.maxwell.af.mil/ warfarestudies/iwac/ IWAC%20PDF/afdd2-5.pdf. Internet. Accessed on 28 April 2002.

Headquarters Department of the Army (HQDA). 1994. Field Manual (FM) 90-29 *Noncombatant Evacuation Operations*. Washington, DC: US Government Printing Office. Available from http://www.adtdl.arm y.mil/cgi-bin/atdl.dll/fm/90-29/Appa.htm. Internet. Accessed on 28 April 2002.

_____. 1995. Army Regulation 530-1, *Operations Security (OPSEC)*. Washington, DC: HQDA.

_____. 1996. Field Manual (FM) 100-6, *Information Operations*. Washington, DC: US Government Printing Office.

Headquarters Department of the Army (HQDA) and Headquarters Marine Corps (HQMC). 1997. Field Manual (FM) 101-5-1/ Marine Corp Reference Publication (MCRP) 5-2A, *Operational Terms and Graphics*. Washington, DC: US Government Printing Office.

Headquarters Marine Corps (HQMC). 1997a. *Concepts and Issues 1997*. Washington, DC: USMC web page. Available from http://www.hqmc.usmc.mil/r-c&i97.nsf/59dc20a8f06587b6852561b70053ca84/5ae5ce1a5cced8ef8525645e0077df83?OpenDocument. Internet. Accessed on 03 May 2002.

_____. 1997b. Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence.* Washington, DC: Marine Corps Doctrine Division web page. Available from https://www.doctrine.usmc.mil/mcdp/ view/mcdp2.pdf. Internet. Accessed on 28 April 2002.

_____. 1998. Marine Corps Order (MCO) 3430.8, *Policy for Information Operations.* Washington, DC: USMC web page. Available from http://www.usmc.mil/directiv.nsf/c535c102facf2e478525651700581759/f294188567c32d398525664b004a8a8a?OpenDocument. Internet. Accessed on 28 April 2002..

_____. 1999. MARADMIN 083/99, *Marine Corps Enterprise Network (MCEN) Circuit Management.* Washington, DC: USMC web page. Available from http://www.usmc.mil/maradmins/maradmin2000.nsf/b21cacd3a24b6f7b852569b9000b19d1/3eac10f0a89100bf85256aab00493a2c?OpenDocument. Internet. Accessed on 28 April 2002.

_____. 2000. *Marine Corps Strategy 21*. Washington, DC: Marine Corps Doctrine Division web page. Available from https://www.doctrine.usmc.mil/Strategy21.htm. Internet. Accessed on 28 April 2002.

_____. 2001a. *Headquarters Marine Corps, Command, Control, Communications, and Computers (C4) Information Assurance.* Washington, DC: USMC web page. Available from http://hqinet001.hqmc.usmc.mil/ c4/ia.htm. Internet. Accessed on 10 December 2001.

_____. 2001b. MARADMIN 439/01, *Information (INFOSEC) and Operations Security (OPSEC) Reminder*. Washington, DC: USMC web page. Available from http://www.usmc.mil/maradmins/maradmin2000.nsf/d50a617f5ac75ae0852568560004f3afc/6f0767f57056532a85256acc000ce2a5?OpenDocument&Highlight=2,439%2F01. Internet. Accessed on 28 April 2002.

_____. 2001c. Marine Corps Capstone Concept: *Expeditionary Maneuver Warfare.* Washington, DC: Marine Corps Doctrine Division web page. Available from https://www.doctrine.usmc.mil/ emw.htm. Internet. Accessed on 28 April 2002.

_____. 2001d. Marine Corps Doctrinal Publication (MCDP) 1-0, *Marine Corps Operations*. Washington, DC: Marine Corps Doctrine Division web page. Available from https://www.doctrine.usmc.mil/ mcdp/vie w/mcdp10.pdf. Internet. Accessed on 28 April 2002.

_____. 2001e. Marine Corps Order (MCO) P1200.7W, *Military Occupational Specialties (MOS) Manual.* Washington, DC: USMC web page. Available from

http://www.usmc.mil/directiv.nsf/9d816d546727ed748525651700581631/4744c049b38f2baf85256af1005cf8fd?OpenDocument. Internet. Accessed on 28 April 2002.

_____. 2001f. *Marine Corps Warfighting Publication (MCWP) 5-1, Marine Corps Planning Process.* Washington, DC: USMC web page. Available from https://www.doctrine.usmc.mil/mcwp/htm/mcwp51.htm. Internet. Accessed on 28 April 2002.

Hyers, Peter. 2000. *Department of the Navy Smart Card: Your Passport to the E-World.* Norfolk, VA: CHIPS Magazine, Summer 2000. Available from http://www.chips.navy.mil/archives/00_jul/smartcard.html. Internet. Accessed on 28 April 2002.

Infowar.Com, Ltd. 1999. *Hamre: Balkans Fighting Called 'First Cyber War'.* St. Petersburg, FL: Infowar.Com, Ltd, web page. Available from http://www.infowar.com/mil_c4i/99/mil_c4i_042399a_j.shtml. Internet. Accessed on 28 April 2002.

Kennedy, Kevin J., Bruce M. Lawlor, and Arne J. Nelson. 1997. *Grand Strategy for Information Age National Security: Information Assurance for the Twenty-first Century.* Maxwell Air force Base, AL: Air University Press.

Lerner, Daniel. 1972. *Propaganda in War and Crisis.* New York, NY: Arno Press.

Luiijf, Eric. 2000. *Information Assurance Under Fire*. London: Information Assurance and data Security SMI conference, Feb 2-3, 2000. Available from http://www.tno.nl/instit/fel/refs/pub2000/smi_luiijf.pdf. Internet. Accessed on 28 April 2002.

Marik, Mary Y. 1998. *Cybercrime…Cyberterrorism…Cyberwarfare…Averting an Electronic Waterloo*. Washington, DC: Center for Strategic and International Studies Press.

Marine Corps Doctrine Division (MCDD). 1997. Marine Corps Concept Paper: *Operational Maneuver From The Sea*. Washington, DC: Marine Corps Doctrine Division posted on the DTIC web page. Availablel from http://www.dtic .mil/jv2020/omfts.pdf. Internet. Accessed on 28 April 2002.

_____. 1998. Marine Corps Concept Paper*: A Concept For Information Operations.* Washington, DC: Marine Corps Doctrine Division web page. Available from https://192.156.75.102/ io.htm. Internet. Accessed on 28 April 2002.

_____. 2001b. Marine Corps Concept Paper (Draft): *A Concept For Information Operations.* Washington, DC: Marine Corps Doctrine Division web page. Available from https://www.doctrine.usmc.mil/IOConcepts/Rev10IOConcept.pdf. Internet. Accessed on 28 April 2002.

Marine Corps Training and Education Command (TECOM). 2002. *United States MarineCorps Organization*. Quantico, VA: TECOM web page. Available from http://www.tecom.usmc.mil/csw/deskguide/ Desktop%20Guide%20-%20United%20States%20 Marine%20Corps%20 Organization.htm. Internet. Accessed on 28 April 200.2.

McNamara, Francis J. 1985. *US Counterintelligence Today*. Washington, DC: The Nathan Hale Institute.

Naval Criminal Investigative Service (NCIS). 2002. *NCIS Counterintelligence*. Washington, DC: NCIS web page. Available from http://www.ncis.navy.mil/ activities/Counterintel/Counterintel.html. Internet. Accessed on 28 April 2002.

Perkins, David D. 1997. Lessons From Bosnia: The IFOR Experience *: IX. Counterintelligence and HUMINT*. Washington, DC: Command and Control Research Program (CCRP), Larry Wentz, (ed.), Office of the Assistant Secretary of Defense (C3I) web page. Available from http://www.dodccrp.org/bosch09.htm. Internet. Accessed on 28 April 2002.

Perkins, Jim. 2000. *Digital War Simmers in the Net.* Washington, DC: Marine Corps News, FAS web page. Available from http://www.fas.org/irp/news/2000/02/ 000228-cyber-usmc.htm. Internet. Accessed on 28 April 2002.

Perry, William J. 1997. *Force Protection*. Madison, AL: ECSI International, Inc. Web Page. Available fromhttp://www.anti-terrorism.com/products/forceprotection.htm. Internet. Accessed on 03 May 2002.

Roberts, Stephen C. 2001. *Information Assurance in the DOD: Static Defense Against the Agile Threat*. Fort Leavenworth, KS: Webster University.

Seltzer, Larry J. 2001. *Password Crackers*. New York, NY: Ziff Davis Media Inc, PC Magazine web page, vol. 21, num. 3, February 12, 2002. Available from http://www.pcmag.com/article/0,2997,s% 253D1481%2526a%253 D19957,00.asp. Internet. Accessed on 28 April 2002.

Shaughnessy, David J. and Thomas M. Cowan. 2001. *Attack on America: The First War of the 21st Century.* Fort Leavenworth, KS: Military Review, US Army Command and General Staff College, Nov-Dec 2001ed. Available from http://www-cgsc.army.mil/milrev/English/Nov-Dec01/pdf/schaugh.pdf. Internet. Accessed on 28 April 2002.

Shulsky, Adam N. 1991. *Silent Warfare*. McLean, VA: Brassey's (US), Inc.

Sullivan, Jr, Julian A. 1991. *Operations Desert Shield and Desert Storm Oral History Interview*. Fort Bragg, NC: US Army Center of Military History web page. Available from http://www.redstone.army.mil/history/ sullivan/welcome.html. Internet. Accessed on 28 April 2002.

Tull, Mark M. 2000. *MAGTF Information Operations*. Quantico, VA: MAGTF Staff Training Program (MSTP), Microsoft Power Point presentation.

Turabian, Kate L. 1996. *A Manual for Writers of Term Papers, Theses, and Dissertation*. 6th ed. Chicago, IL: The University of Chicago Press.

Verton, Daniel. 2000. Pentagon budget guided by Kosovo lessons. Falls Church, VA: Federal Computer Week Media Group, Federal Computer Week web page. Available from http://www.fcw.com/fcw/articles/ 2000/0207/web-kosovo-budget-02-09-00.asp. Internet. Accessed on 28 April 2002.

Villahermosa, Gilberto. (n.d.). *Desert Storm: The Soviet View*. Fort Leavenworth, KS: Foreign Military Studies Office, FAS web page. Available from http://www.fas.org/man/dod-101/ops/docs/rs-storm.htm. Internet. Accessed on 28 April 2002.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
   U.S. Army Command and General Staff College
   250 Gibbon Ave.
   Fort Leavenworth, KS 66027-2314

2. Defense Technical Information Center/OCA
   825 John J. Kingman Rd., Suite 944
   Fort Belvoir, VA 22060-6218

3. Marine Corps Staff College
   Breckenridge Library
   MCCDC
   Quantico, VA 22134

7. Richard W. Snyder, LtCol, USAF
   Directorate of Joint and Multinational Operations
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

8. Anthony McNeill, LtCol, USMC
   Marine Element
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 31 May 2002

2. Thesis Author:

3. Thesis Title:

4. Thesis Committee Members _____

   Signatures: _____

   _____

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

(A) B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

EXAMPLE

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
Direct Military Support (10)	/	Chapter 3	/	12
Critical Technology (3)	/	Section 4	/	31
Administrative Operational Use (7)	/	Chapter 2	/	13-32

Fill in limitation justification for your thesis below:

Limitation Justification Statement	/	Chapter/Section	/	Page(s)
	/		/	
	/		/	
	/		/	
	/		/	
	/		/	

7. MMAS Thesis Author's Signature: _____

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).