

MARINE AIR-GROUND TASK FORCE OFFENSIVE INFORMATION
OPERATIONS, SUPPORTING OPERATIONAL
MANEUVER FROM THE SEA

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
Strategy

by

SCOTT D. AIKEN, MAJ, USMC
B.S., Vanderbilt University, Nashville, Tennessee, 1985
M.P.A., Troy State University, Troy, Alabama, 1998

Fort Leavenworth, Kansas
2000

Approved for public release; distribution is unlimited.

20001120 037

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

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

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE <p style="text-align: center;">2 Jun 00</p>	3. REPORT TYPE AND DATES COVERED <p style="text-align: center;">Master's Thesis 6 Aug 99--2 Jun 00</p>	
4. TITLE AND SUBTITLE Marine Air-Ground Task Force Offensive Information Operations, Supporting Operational Maneuver from the Sea		5. FUNDING NUMBERS	
6. AUTHOR(S) Major Scott D. Aiken, USMC			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) U.S. Army Command and General Staff College ATTN: ATZL-SWD-GD 1 Reynolds Ave. Ft. Leavenworth, KS 66027-1352		8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/ MONITORING AGENCY NAME(S) AND ADDRESS(ES)		10. SPONSORING/MONITORING	
11. SUPPLEMENTARY NOTES			
12a. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.		12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 words) The Marine Air-Ground Task Force (MAGTF) is the organizational structure that the Marine Corps will continue to use to task organize forces. The Marine Corps must prepare doctrine to meet the challenges and opportunities that Information Operations (IO) offers. The challenges and opportunities of IO are only now beginning to be defined by the Marine Corps. Currently, there is no Marine Corps doctrine to assist MAGTF personnel in the conduct of offensive IO. This thesis proposes thirteen doctrinal principles for the employment of the elements of offensive IO for a forward deployed MAGTF operating in a littoral, unformed or developing operational environment. These proposed doctrinal principles support Operational Maneuver From the Sea and provide a link between the 1998 Marine Corps Concept Paper <i>A Concept for Information Operations</i> and actual operating procedures. These proposed doctrinal principles are more specific than current Joint doctrine. This thesis also proposes several recommendations for the implementation of these principles into procedure. The documentary (historical) method and the case studies, based on successful historical examples of operations in the littorals from World War II to the present, are used.			
14. SUBJECT TERMS Marine Air-Ground Task Force (MAGTF), Offensive Information Operations, Operational Maneuver from the Sea, MEU		15. NUMBER OF PAGES 145	16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

MARINE AIR-GROUND TASK FORCE OFFENSIVE INFORMATION
OPERATIONS, SUPPORTING OPERATIONAL
MANEUVER FROM THE SEA

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
Strategy

by

SCOTT D. AIKEN, MAJ, USMC
B.S., Vanderbilt University, Nashville, Tennessee, 1985
M.P.A., Troy State University, Troy, Alabama, 1998

Fort Leavenworth, Kansas
2000

Approved for public release; distribution is unlimited.

MASTER OF MILITARY ART AND SCIENCE

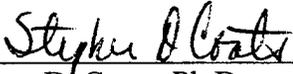
THESIS APPROVAL PAGE

Name of Candidate: Major Scott D. Aiken, USMC

Thesis Title: Marine Air-Ground Task Force Offensive Information Operations,
Supporting Operational Maneuver from the Sea

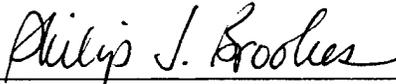
Approved by:


_____, Thesis Committee Chairman
Lieutenant Colonel Frederic W. Lickteig, M.S.


_____, Member
Stephen D. Coats, Ph.D.


_____, Member
Lieutenant Commander Gregory M. Landis, B.S.

Accepted this 2d day of June 2000 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

MARINE AIR-GROUND TASK FORCE OFFENSIVE INFORMATION OPERATIONS, SUPPORTING OPERATIONAL MANEUVER FROM THE SEA, by Major Scott D. Aiken, USMC, 114 pages.

The Marine Air-Ground Task Force (MAGTF) is the organizational structure that the Marine Corps will continue to use to task organize forces. The Marine Corps must prepare doctrine to meet the challenges and opportunities that Information Operations (IO) offers. The challenges and opportunities of IO are only now beginning to be defined by the Marine Corps. Currently, there is no Marine Corps doctrine to assist MAGTF personnel in the conduct of offensive IO.

This thesis proposes thirteen doctrinal principles for the employment of the elements of offensive IO for a forward deployed MAGTF operating in a littoral, unformed or developing operational environment. These proposed doctrinal principles support Operational Maneuver From the Sea and provide a link between the 1998 Marine Corps Concept Paper *A Concept for Information Operations* and actual operating procedures. These proposed doctrinal principles are more specific than current Joint doctrine. This thesis also proposes several recommendations for the implementation of these principles into procedure.

The documentary (historical) method and the case studies, based on successful historical examples of operations in the littorals from World War II to the present, are used.

ACKNOWLEDGMENTS

First, I would like to thank my parents, Mr. and Mrs. Luther L. Aiken of Nashville, Tennessee, for thirty-six years of constant support. Second, I want to thank my committee, Lieutenant Colonel Fred Lickteig, USMC; Doctor Stephen D. Coats; and Lieutenant Commander Greg M. Landis, USN. I appreciate your guidance and direction. Finally, I would like to thank the Staff of the Combined Arms Research Library (CARL) at Fort Leavenworth, Kansas. Your research expertise and dedication to customer service is outstanding.

This thesis is dedicated to the most potent and flexible weapon in the United States arsenal--the Marine. I hope it helps when the next call to "land the landing force" is heard. Semper Fi, Mac.

TABLE OF CONTENTS

	Page
APPROVAL PAGE	ii
ABSTRACT	iii
ACKNOWLEDGMENTS	iv
LIST OF ABBREVIATIONS	vi
LIST OF FIGURES	x
LIST OF TABLES	xi
CHAPTER	
ONE. INTRODUCTION	1
TWO. DEFINITION OF INFORMATION OPERATIONS	16
THREE. THREAT ANALYSIS	23
FOUR. HISTORICAL EXAMPLES OF INFORMATION OPERATIONS	35
FIVE. CONCLUSIONS AND RECOMMENDATIONS	89
APPENDIX	
A. DEFINITIONS	115
B. ADDITIONAL HISTORICAL EXAMPLES	118
REFERENCE LIST.....	123
INITIAL DISTRIBUTION LIST	130

LIST OF ABBREVIATIONS

AAAV	Advanced Amphibious Assault Vehicle
ACE	Aviation Combat Element
AFDD	Air Force Doctrine Document
APOD	Air Port of Debarkation
ARG	Amphibious Ready Group
BOS	Battlefield Operating System
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
CAS	Close Air Support
CATF	Commander, Amphibious Task Force
CERT	Computer Emergency Response Team
CI	Counterintelligence
CIA	Central Intelligence Agency
CINC	Commander-In-Chief
CINCUSSPACECOM	Commander-In-Chief, United States Space Command
CLF	Commander, Landing Force
CNA	Computer Network Attack
DoD	Department of Defense
EA	Electronic Attack

E-Commerce	Electronic Commerce
E-Mail	Electronic Mail
EP	Electronic Protection
EPW	Enemy Prisoner of War
ES	Electronic Warfare Support
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FM	Field Manual
IA	Information Assurance
INSS	Institute for National Strategic Studies
IO	Information Operations
IPB	Intelligence Preparation of the Battlefield
IW	Information Warfare
JCIWS	Joint Command, Control, and Information Warfare School
JFC	Joint Force Commander
JTF	Joint Task Force
KTO	Kuwaiti Theater of Operations
LCAC	Landing Craft, Air Cushioned
MAGTF	Marine Air-Ground Task Force
MCDP	Marine Corps Doctrinal Publication
MCPP	Marine Corps Planning Process
MCIA	Marine Corps Intelligence Activity
MCO	Marine Corps Order

MCRP	Marine Corps Reference Publication
MCWP	Marine Corps Warfighting Publication
MEB	Marine Expeditionary Brigade
MEF	Marine Expeditionary Force
MEU	Marine Expeditionary Unit
MEU (SOC)	Marine Expeditionary Unit (Special Operations Capable)
MOOTW	Military Operation Other Than War
MTT	Mobile Training Team
NATO	North Atlantic Treaty Organization
OMFTS	Operational Maneuver from the Sea
OPSEC	Operations Security
PDF	Panamanian Defense Force
PSYOP	Psychological Operations
SATCOM	Satellite Communications
SIO	Special Information Operations
SOF	Special Operations Forces
SOPs	Standing Operating Procedures
SOUTHCOM	Southern Command
SPMAGTF	Special Purpose MAGTF
TBM	Theater Ballistic Missile
TTPs	Techniques, Tactics and Procedures
USAF	United States Air Force

V/STOL

Vertical/Short Takeoff and Landing

WMD

Weapons of Mass Destruction

LIST OF FIGURES

Figure	Page
1. Elements of Information Operations	20
2. Operational Environments	25
3. Basic Five Rings Model	65

LIST OF TABLES

Table	Page
1. Principles of Offensive Information Operations	2
2. Principles of OMFTS	14
3. Steps of Research Methodology	15
4. Elements of Offensive IO, Marine Corps Concept Paper and Joint Publication 3-13 Compared	21
5. Threats to a MAGTF, Matrixed	33
6. Historical Examples for Each Element of Offensive IO	37
7. Combined Use of the Elements of Offensive IO, Faylaka Island	40
8. Combined Use of the Elements of Offensive IO, Operation Pastel	48
9. Deception Operations in Support of Operation Overlord	50
10. Operation Just Cause H-Hour Targets	63
11. Combined Use of the Elements of Offensive IO, Operation Just Cause	66
12. Results of Operation El Dorado Canyon	71
13. Combined Use of the Elements of Offensive IO, Operation El Dorado Canyon	73
14. Conduct of a Distributed Denial of Service Attack	78
15. Combined Use of the Elements of Offensive IO, The Attack against Admiral Yamamoto	85
16. Time and Command	106
17. Notional Critical Target Sets	108
18. Proposed Doctrinal Principles in the Employment of Offensive IO by the MAGTF	112

19. Additional Historical Examples, PSYOP	118
20. Additional Historical Examples, Deception	119
21. Additional Historical Examples, OPSEC	120
22. Additional Historical Examples, EW	120
23. Additional Historical Examples, CNA	121
24. Additional Historical Examples, SIOs	122

CHAPTER ONE

INTRODUCTION

Background

The ability to conduct offensive Information Operations (IO) across the spectrum of conflict in the future is critical to the success of the Marine Corps for two reasons. First, offensive IO will be a force multiplier for deployed forces, which by mobility requirements and resource shortages, are austere and lean by nature. Second, offensive IO may prove to be very effective against the myriad of existing and emergent threats, with their increased lethality and reliance on asymmetrical warfare.

The Marine Air-Ground Task Force (MAGTF) is the organizational structure that the Marine Corps will continue to use to task organize forces. The Marine Corps must prepare doctrine to meet the challenges and opportunities that IO offers. The challenges and opportunities of IO are only now beginning to be defined by the Marine Corps. Currently, there is no Marine Corps doctrine to assist MAGTF personnel in the conduct of offensive IO.

Additionally, the existing principles of offensive IO found in Joint Publication 3-13, *Joint Doctrine for Information Operations*, as listed in table 1, are general in nature. They do not adequately address the complexities of conducting IO in the environment where the Marine Corps will be called upon to conduct operations: in a littoral region with an unformed or developing operational environment.

Table 1.

Principles of Offensive Information Operations.

The human decision making processes are the ultimate target for offensive IO. Offensive IO requires the integration and coordination of various capabilities.
Offensive IO objectives must be clearly established, support overall national and military objectives, and include identifiable indicators of success.
Selection and employment of specific offensive capabilities against an adversary must be appropriate to the situation and consistent with U.S. objectives.
Offensive IO may be the main effort, a supporting effort, or a phase of a joint force commander's (JFC's) campaign or operation.
Offensive IO in support of a JFC's campaign or operation may include planning and execution by non-Department of Defense (DoD) forces, agencies, or organizations and must be thoroughly integrated, coordinated, and deconflicted with all other aspects and elements of the supported campaign or operation.
To efficiently attack adversary information and information systems, it is necessary to be able to: <ul style="list-style-type: none">• Understand the adversary's perspective and how it may be influenced by IO.• Establish IO objectives.• Identify information systems value, use, flow of information, and vulnerabilities.• Identify targets that can help achieve IO objectives.• Determine the target set.• Determine the most effective capabilities for affecting the vulnerable portion of the targeted information or information systems.• Predict the consequences of employing specific capabilities with a predetermined level of confidence.• Obtain necessary approval to employ IO.• Identify intelligence and combat information feedback necessary to support assessment.• Integrate, coordinate, and implement IO.• Evaluate the outcome of specific IO.

Source: The Joint Chiefs of Staff. Joint Publication 3-13, *Joint Doctrine for Information Operations*. Washington, DC: The Joint Staff, 9 October 1998, II-1 and II-2.

Marine Corps IO doctrine should include guidance on the integration of offensive IO into the planning and execution of all MAGTF offensive operations throughout the spectrum of warfare. This doctrine should include the operational level of war, but

emphasize the tactical level of war. The operational and tactical levels of war are the levels of war that are executed by deployed MAGTFs in an unformed or developing operational environment. This doctrine should be applicable for all types and sizes of MAGTFs, including Special Purpose MAGTFs (SPMAGTFs), Marine Expeditionary Units (MEUs), Marine Expeditionary Brigades (MEBs) and Marine Expeditionary Forces (MEFs).

The lack of offensive IO doctrine is occurring at a very critical time in history. The Information Age is ensuring that there is a proliferation of the knowledge, equipment and means to attack the world's dominant military power, the United States. The collapse of the bipolar world, the rise of ambitious regional powers, and the expanding gap between the "have's" and the "have-not's" will provide the United States with an ever-increasing number of asymmetrical threats and chaotic situations along the lower end of the spectrum of conflict. All this will occur while the U.S. military must still remain vigilant and ready for conflicts of medium-to-high intensity. Conversely, the Information Age opens up vast opportunities to develop and execute offensive IO against our adversaries. The importance of these challenges and opportunities warrants further study.

The increased challenges and opportunities provided by geopolitical factors and technologies in the field of IO have led to their study by the U.S. military. Some joint and service doctrine exists. However, planners are hard-pressed to keep up with the extremely rapid pace of technology. Offensive IO, in relation to the MAGTF, needs to be studied in greater detail. Such study would be an attempt to bridge the gap between the concepts and execution of offensive IO. These IO would take place in executing

Operational Maneuver from the Sea (OMFTS), which is the Navy and Marine Corps' approach to current and future expeditionary, littoral and amphibious warfare.

Purpose

The U.S. Navy and Marine Corps have conducted a great deal of research in updating and improving expeditionary, littoral and amphibious warfare capabilities for the future. Much of this research has been in the form of advanced technology to keep pace with the increasingly lethal threats and technological advances throughout the world. Examples include the amphibious triad of the advanced amphibious assault vehicle (AAAV), the Vertical/Short Takeoff and Landing (V/STOL) transport (MV-22 Osprey), and the landing craft, air cushioned (LCAC). The time has come to match this technical research with research designed to provide improved, coordinated offensive IO capabilities for the MAGTF.

Research Question

The purpose of this work is to study the possible use of offensive IO by the MAGTF. The primary research question for this thesis is: What are the doctrinal principles that will enable the MAGTF to conduct offensive Information Operations in a littoral region with an unformed or developing operational environment? This question will be answered by a historical research methodology.

Definition of Doctrinal Principle

As a point of clarification, Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, defines "doctrine" as "the fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application."

Webster's Dictionary defines "principle" as a "general or fundamental law." The doctrinal principles recommended in this thesis will adhere to this definition.

Subordinate Questions

There are several related subordinate questions that must be answered in this thesis to address the MAGTF's ability to conduct offensive IO in littoral regions representing an unformed or developing operational environment. These subordinate questions include:

1. What are the elements of IO in accordance with the current Marine Corps Concept Paper on Information Operations? These questions are answered in chapter two of this thesis.
2. What are the existing and emerging threats to the MAGTF's ability to conduct offensive operations in the future? This question is answered in chapter three.
3. Based on historical examples, what are general trends of IO that can generate proposed doctrinal principles offensive IO for use by the MAGTF? What are these proposed doctrinal principles? Are they still relevant? Are the doctrinal principles of IO shown by the selected historical examples feasible for use by a future MAGTF? Will the doctrinal principles of IO shown by the selected historical examples add to the combat power of the MAGTF? If so, how? These questions are answered in chapters four and five.
4. What are the most necessary and/or useful elements of offensive IO for a MAGTF? This question is answered in chapter five.

Definitions

Several operational definitions are clarified for use in the thesis. These definitions are found in appendix A, "Definitions." (The definitions of elements of Information Operations, Information Operations, Information Warfare and Offensive IO are found in chapter two, "Definition of Information Operations.")

Assumption

One assertion made at the start of this research was that although IO is a relatively new concept, warriors have long since been using the elements of IO to gain an advantage on the battlefield. The assumption is made that history will provide us with examples from which trends can be seen and doctrinal principles of offensive IO can be found for use by the MAGTF commander and staff of a deployed MAGTF in a littoral region with an unformed or developing operational environment.

Limitations

One limitation to this research is the inability of researchers and writers to keep up with the increasingly rapid pace of the development of IO threats and opportunities, particularly in an unclassified forum. Another limitation is the inability to clearly determine IO threats. A plethora of threats exist, both in form and actor. However, because of their latent nature, they may only be discovered once their action is complete. This thesis determined and concentrated on those threats that are particularly dangerous to MAGTFs. Conversely, a fourth limitation is the vast numbers of opportunities in the field of offensive IO. This thesis addresses those opportunities that are particularly suited for execution by deployed MAGTFs, in littoral regions, during the initial days of a contingency.

Delimitations

There are several delimitations on the scope of this research to maintain its feasibility and focus. These delimitations include:

1. This thesis only covers MAGTF operations.
2. This thesis only focuses on proposed doctrinal principles, proposed techniques, tactics, and procedures (TTPs) are the subject of future research.
3. This thesis only covers the most dangerous and likely threats to a MAGTF's ability to conduct offensive operations, which can span the spectrum of conflict, other published works cover the myriad of threats in greater detail.
4. Because of the vast amount of historical examples available, this thesis only uses historical examples that have occurred in littoral regions during and after World War II. This delimitation allows for the study of the impact of modern technology on what would now be considered IO.
5. This thesis only covers offensive IO doctrine that is achievable by deployed MAGTFs, defensive IO doctrine is the subject of further research. (This is contrary to the guidance issued by the Joint Command, Control, and Information Warfare School (JCIWS), but it necessary to maintain the scope of this thesis (Joint Command, Control, and Information Warfare School 2000, I-2).
6. The thesis covers MAGTF IO in a littoral environment, centered on amphibious power projection in an unformed or developing operational environment. IO during later phases of an operation will be conducted by the JFC.

7. This thesis only covers doctrine that can potentially be used through the year 2010, based on estimates of technological advances; this coincides with *Joint Vision 2010* and OMFTS.
8. This thesis does not consider the moral or legal aspects of executing IO.
9. This thesis is unclassified.

Initial Research Design

Research design for this thesis is based on the historical approach and follows the following steps:

- Step 1: The term “Information Operations” is defined.
- Step 2: Threat identification and analysis.
- Step 3: Historical examples of IO are studied
- Step 4: MAGTF offensive IO analysis
- Step 5: Recommended doctrinal concepts

Significance of Study

This thesis is significant in that it proposes new offensive IO doctrinal principles to increase the deterrence capability, flexibility and overall combat power of the MAGTF. These principles are more specific than current joint doctrine and are based on successful historical examples.

Literature Review

The Marine Corps’ research in the development of its warfighting doctrine, centered on maneuver warfare as contained in Marine Corps Doctrinal Publication 1 *Warfighting*, has provided its operating forces a solid, proven method of warfare for the future. This doctrine is suitable for the entire spectrum of warfare. It was validated in

Operations Desert Shield and Desert Storm and every contingency since. Proposed doctrinal principles for offensive IO by MAGTFs must use this doctrine as a precept to any proposed offensive IO doctrine.

Operational concepts such as OMFTS and its supporting concepts, are an attempt to integrate technology with doctrine. OMFTS, as well as the Marine Corps' concept on IO, have not yet bridged the gap between technology, doctrine or emerging threats.

This gap leads back to the proposed primary research question: "What are the doctrinal principles that will enable the MAGTF to conduct offensive Information Operations in a littoral region with an unformed or developing operational environment?" This thesis studies this question and provides input to the Marine Corps with proposed doctrinal principles to assist MAGTF personnel in the conduct of offensive IO.

There are currently two authoritative works in the field of Information Operations for the Marine Corps. The first authoritative work is Marine Corps Order (MCO) 3430.8, "Policy for Information Operations." It is a 1997 document that outlines definitions, provides initial guidance, and establishes responsibilities for IO within the Marine Corps.

The capstone doctrinal concept to support the Joint Chiefs of Staff's *Joint Vision 2010* and the Department of the Navy's *Forward . . . from the Sea is Operational Maneuver from the Sea, A Concept for the Projection of Naval Power Ashore*. This concept paper outlines the "marriage" between maneuver warfare and naval warfare. Twelve supporting concepts have since been developed to support the Operational Maneuver from the Sea concept, with two more in development. Of these, one, *A Concept for Information Operations*, was published in May 1998. This supporting concept paper is a second authoritative work and is an attempt by the Marine Corps to

broadly show how IO will support OMFTS. This thesis makes the assumption that *A Concept for Information Operations* is the future direction of the Marine Corps and use its contents as authoritative. This concept paper gives the general guidance and direction for further IO doctrinal development. It also provides a conceptual link to OMFTS.

Supporting these two authoritative works is the Marine Corps Intelligence Activity's (MCIA's) excellent *Midrange Threat Estimate 1997-2007: Finding Order in Chaos*. This estimate serves as the baseline for the threat analysis found in chapter three of this thesis. Another important supporting work for threat analysis is the *Strategic Assessment 1999: Priorities for a Turbulent World*, by the Institute for National Strategic Studies (INSS) of the National Defense University.

Key works for this topic include six joint publications, two Army field manuals, and one Air Force doctrinal document. The six joint publications that pertain to the topic include *Joint Doctrine for Amphibious Operations* (Joint Publication 3-02), *Joint Doctrine for Information Operations* (Joint Publication 3-13), *Joint Doctrine for Command and Control Warfare* (Joint Publication 3-13.1), *Joint Doctrine for Psychological Operations* (Joint Publication 3-53), *Joint Doctrine for Operational Security* (Joint Publication 3-54), and *Joint Doctrine for Military Deception* (Joint Publication 3-58). Army Field Manual 100-6, *Information Operations*, Army Field Manual 33-1, *Psychological Operations*, and Air Force Doctrine Document 2-5, *Information Operations* are also extremely relevant to this topic.

Numerous historical references were used in this thesis to provide the littoral examples. Each reference was chosen because of the author's value as a primary source

or subject matter expert. Several historical references were used for each example, to provide collaborating facts and analysis of the event.

Research Design

As stated earlier, research design for this thesis is based on the historical method. This method is described by David J. Fox in *The Research Process in Education* and Tyrus Hillway in *Introduction to Research, Second Edition*. This research process of this thesis follows five steps.

The first step is to clarify the definition of IO in the context of *A Concept for Information Operations*. Since that paper was written before Joint Publication 3-13, there are some gaps in continuity and common terminology. Recommendations to the Marine Corps for revising the IO concept paper to reflect Joint Publication 3-13 are provided.

Second, the thesis uses MCIAs' *Midrange Threat Estimate 1997-2007: Finding Order in Chaos* as a base line to study the current and future potential threats that the MAGTF may have to face across the spectrum of conflict. An unclassified analysis is conducted on threats that may be present in 2010. Current open source intelligence studies were used in this analysis. These threats are examined across the spectrum of conflict, to include their IO capabilities. As stated earlier, this thesis concentrates on those threats that are particularly dangerous to a MAGTF's ability to conduct offensive operations. Evaluation of those threats are based on the two following sets of threat identification and analysis criteria:

Force and time based set of criteria. (Subsets include threats to a MAGTF while underway, threats to a MAGTF inside the littoral battlespace, and threats to a MAGTF

ashore.) In their Midrange Threat Analysis, MCI developed this set of criteria, which was modified by the author into the three subsets shown above.

Threats as defined by the severity of their potential consequences. This set of criteria was developed by Richard O. Hundley and Robert H. Anderson in their essay “Emerging Challenge: Security and Safety in Cyberspace” part of *In Athena’s Camp, Preparing for Conflict in the Information Age* by John Arquilla and David Ronfeldt.

The third step of the research process is to study historical examples of IO. As stated by Lord Lytton, “If you want a good idea, read an old book” (Luvaas 1982, 20). History has numerous examples of past uses of what would now be considered IO. This thesis uses two of Hillway’s four methods of research, the documentary (historical) method, and the case study (Hillway 1964, 137). Criteria for selection of these historical examples included the following:

1. The historical example was an operation that occurred in a littoral environment.
2. The historical example took place during or after World War II.
3. The historical example is a forerunner of what today would be considered an element of offensive IO.
4. The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future.
5. Two examples per element of offensive IO were used.

These historical examples were analyzed based on the following criteria:

1. Are the doctrinal principles shown by these historical examples still relevant? Have they been overcome by technology? Will they prove useful to present and emerging threats?

2. Are the doctrinal principles shown by these historical examples feasible for use by a MAGTF in the future?
3. Will the doctrinal principles shown by these historical examples add to the combat power of the MAGTF?

The fourth step of the research process was to use the previous historical examples to study the ways in which MAGTFs can exploit offensive IO across the spectrum of warfare in the future. As stated by Leedy, "Events do crystallize into meaningful clusters" (Leedy 1989, 125). Common doctrinal trends were sought throughout the historical examples. This research also determined the elements of IO that are most useful for MAGTFs in the future. It is expected that these elements vary in relation to the intensity of conflict. Additionally, this research identifies shortfalls in elements of offensive IO and makes recommendations on whether to research these areas further, allocate resources to counter the threats, or rely on other services for support. Criteria used to evaluate proposed doctrinal principles and determine the most necessary and/or useful elements include comparing them to the principles of OMFTS shown in table 2. Existing joint doctrinal principles also serve as criteria for the evaluation of proposed doctrinal principles to ensure consistency.

Offensive IO doctrine remains the same through the spectrum of conflict, doctrinal principles for littoral operations are proposed. However, the use of the elements of IO vary in relation to the intensity of conflict and in relation to the command and control capability of the target.

Table 2.

Principles of OMFTS.

Focuses on an operational objective
Uses the sea as maneuver space
Generates overwhelming combat power
Pits strength against weakness
Emphasizes intelligence, deceptions, and flexibility
Integrates all organic, joint, and combined operations

Source: Headquarters, United States Marine Corps. *Operational Maneuver from the Sea, A Concept for the Projection of Naval Power Ashore*. Washington, DC: United States Marine Corps, June 1996. 6.

Finally, this thesis develops and provides recommended courses of action with regard to offensive IO in relation to the MAGTF. These recommended courses of action include elements of IO to emphasize, elements of IO to rely on other services for support, and recommended doctrinal principles. According to Marine Corps Doctrinal Publication 1, *Warfighting*, doctrine is a:

teaching of the fundamental beliefs of the Marine Corps on the subject of war, from its nature and theory to its preparation and conduct. Doctrine establishes a particular way of thinking about war and a way of fighting. It also provides a philosophy for leading Marines in combat, a mandate for professionalism, and a common language. In short, it establishes the way we practice our profession. In this manner, doctrine provides the basis for harmonious actions and mutual understanding. . . . Our doctrine does not consist of procedures to be applied in specific situations so much as it sets forth general guidance that requires judgment in application. Therefore, while authoritative, doctrine is not prescriptive. (Headquarters, United States Marine Corps 1997b, 55-56)

The recommended doctrinal principles will provide MAGTF leadership and staff with the “basis for harmonious actions and mutual understanding” needed in the area of offensive IO in a littoral region with an unformed or developing operational environment.

In summary, Fox breaks the actual process of historical research into the nine major steps listed in table 3. This table is modified to compare Fox's research steps with the steps conducted in this thesis.

Table 3.
Steps of Research Methodology.

Step	Action
1	Determination that the problem selected is appropriate for study through the historical approach (conducted informally in this thesis)
2	Specification of the population of data needed (use of delimits)
3	Initial determination that sufficient data are available (conducted informally in this thesis)
4	Begin data collection through: <ul style="list-style-type: none"> • Consideration of known data • Seeking new data from known sources (primary, secondary sources) • Seeking new and previously unknown data (in the form of data, in the form of sources) (Step 3 of this thesis' research process)
5	Begin to write report
6	Interaction of writing and additional search for data or examination of data
7	Completion of descriptive phase of research
8	Completion of interpretative phase of research (Step 4 of this thesis' research process)
9	Application of data to present and hypotheses for the future (Step 5 of this thesis' research process)

Source: Fox, David J. 1969. *The Research Process in Education*. New York: Holt, Rinehart and Winston, Inc., 416.

CHAPTER TWO

DEFINITION OF INFORMATION OPERATIONS

The purpose of this chapter is to answer the first subordinate question, which is: What is IO? Additionally, the follow-on question: What are the elements of offensive IO in accordance with the Marine Corps concept paper? will be answered. A tertiary question to be answered is: Should elements of offensive IO be added or subtracted in accordance with joint and other service doctrine? This chapter defines “information operations” in accordance with the current authoritative work for the Marine Corps, *A Concept for Information Operations*. While the definition of IO is consistent throughout most of the joint and service publications, the elements that are considered as part of IO are not. The elements of IO in accordance with the concept paper are not consistent with joint doctrine as found in Joint Publication 3-13, *Joint Doctrine for Information Operations*. Inconsistencies can be attributed in part to the concept paper being released in May 1998, which is five months before Joint Publication 3-13’s 9 October 1998 publish date and the overall rapid evolution of thought in all topics related to IO.

As contained in MCO 3430.8, “Policy for Information Operations,” a 1997 Marine Corps definition for IO was “Actions taken to affect adversary information and information systems while defending one’s own information and information systems” (Headquarters, United States Marine Corps 1997a, 2). This is the same definition as contained in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* (23 March 1994, as amended through 9 April 1997), and Joint Publication 3-13, *Joint Doctrine for Information Operations* (Headquarters, United States

Marine Corps 1997a, 2). Only Field Manual 101-5-1 (Marine Corps Reference Publication 5-2A), *Operational Terms and Graphics*, of 1997 defines IO differently, with a more encompassing definition of:

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. (Headquarters, Department of the Army 1997, 1-82)

Surprisingly, the 1997 definition for IO from MCO 3430.8 is still used in *A*

Concept for Information Operations! No evolution of the definition is apparent.

Excerpts from the concept paper do describe IO, stating that IO is

an integrating concept that facilitates the warfighting functions of command and control, fires, maneuver, logistics, intelligence, and force protection, not simply another "arrow" in the MAGTF commander's quiver. It is, rather, a broad-based capability that "makes the bow stronger."

The paper further states,

IO exploit opportunities--and minimize vulnerabilities--inherent to dependence on the information that supports military activities. They include actions taken in the information environment by Marine forces to achieve specific results against potential adversaries and are conducted across the full range of military operations. IO target decision makers, information-dependent systems (including weapons), infrastructure, command and control, computers, and associated network systems will play a critical role in supporting the military operations envisioned in Marine Corps warfighting concepts. (Marine Corps Combat Development Command 1998, 1)

For the purposes of this thesis the definition of IO as contained in MCO 3430.8 and the concept paper is used.

In this thesis, the definition of IO is briefly compared to command and control warfare (C2W) and information warfare (IW). MCO 3430.8 defines C2W as "The integrated use of Operations Security (OPSEC), Military Deception, Psychological

Operations (PSYOP), Electronic Warfare (EW) and Physical Destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary Command and Control (C2) capabilities, while protecting friendly capabilities against such actions” (Headquarters, United States Marine Corps 1997a, 1). Joint Publication 3-13 rephrases the definition by stating “C2W is application of IO in military operations that specifically attacks and defends the C2 target set” (The Joint Chiefs of Staff 1998, I-4). Joint Publication 3-13 further states that C2W is both offensive and defensive. As is seen later, this definition aligns with the elements of offensive and defensive IO in accordance with *A Concept for Information Operations*. This thesis, therefore, considers C2W a subset of IO.

MCO 3430.8 defines Information Warfare as “IO conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries” (MCO 3430.8 1997, 1). This definition is broad, and implies offensive action. This is the same definition that is found in Joint Publications 1-02 and 3-13. FM 100-5-1, *Operational Terms and Graphics*, defines IW as “Actions taken to achieve information superiority by affecting a hostile’s information, information-based processes and information systems, while defending one’s own information, information-based processes and information systems” (Headquarters, Department of the Army 1997, 1-82). This definition is broader than the first definition of IW, and specifically sets “information superiority” as a goal. This later definition is closer to the current definition of IO. Therefore, this thesis considers IW roughly equivalent to IO.

The elements, subcategories of IO, as defined by the Marine Corps (*A Concept for Information Operations* concept paper), are as follows:

1. Offensive Information Operations: Includes computer network attack (limited Marine Corps role) and command and control warfare, which includes psychological operations, deception, operations security, physical destruction and electronic warfare (electronic attack, support, protection).
2. Defensive Information Operations: Includes physical security, information assurance, counter-psychological operations, counter-deception, operations security, electronic protection, counterintelligence and counterreconnaissance.
3. Civil Affairs
4. Public Affairs (Marine Corps Combat Development Command 1998, 4-5)

Figure 1 graphically portrays these elements.

Although not specifically defined by either MCO 3430.8 or *A Concept for*

Information Operations, the concept paper does state the following about offensive IO:

MAGTFs will conduct offensive IO primarily at the operational and tactical levels to deny or disrupt the adversary's use of information and information systems. The MAGTF commander may utilize electronic attack, physical destruction, psychological operations, and/or deception to prosecute targets related to command and control, intelligence, and other critical information-based processes directly related to conducting military operations. A principal focus of offensive IO at this level is the enemy commander and his decision making process. By targeting the human element, we seek to affect the adversary's will to resist. The MAGTF commander's intent is paramount; all elements of MAGTF IO must work together to produce a synergistic effect. (Marine Corps Combat Development Command 1998, 6)

Offensive IO, as defined by Joint Publication 3-13, is "the integrated use of assigned and supporting capabilities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives" (The Joint Chiefs of Staff 1998, GL-9). Joint doctrine states that offensive IO includes operational security (OPSEC), military deception, psychological operations, electronic warfare (EW), physical attack/destruction, and special information operations (SIO), and may include computer network attack.

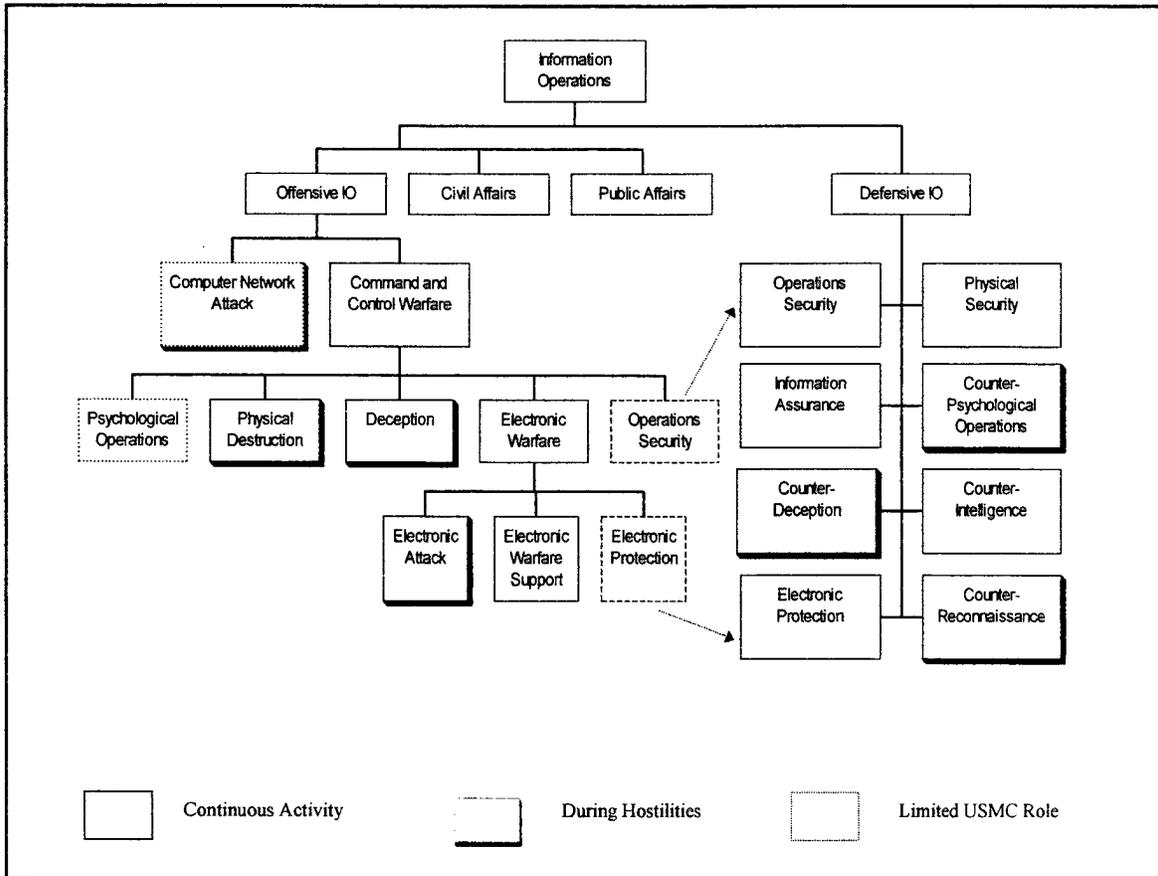


Figure 1. Elements of Information Operations. Marine Corps Combat Development Command. *A Concept for Information Operations*. Quantico, Virginia: United States Marine Corps, 15 May 1998, 4-5.

While the joint definition is closely aligned with *A Concept for Information Operations*, inconsistencies exist between joint doctrine and the concept paper as to the elements of offensive IO. Such inconsistencies can lead to lack of coordination, duplication of effort, and can reduce the effectiveness of the joint IO effort. In future resource-constrained environments, this could mean the difference between success and failure.

The inconsistencies that exist between joint doctrine and the Marine Corps concept paper as to the elements of offensive IO are shown in table 4 below.

Table 4.

Elements of Offensive IO, Marine Corps Concept Paper and Joint Publication 3-13 Compared.

Marine Corps Concept Paper	Joint Publication 3-13
1. Psychological Operations	1. Psychological Operations
2. Deception	2. Military Deception
3. Operations Security	3. Operational Security
4. Physical Destruction	4. Physical Attack/Destruction
5. Electronic Warfare (attack, support, protection)	5. Electronic Warfare (EW)
6. Computer Network Attack (limited Marine Corps role)	6. Special Information Operations (SIO) 7. may include Computer Network Attack

Both sources state that Computer Network Attack (CNA) may be used in offensive IO. With the Commander-In-Chief, United States Space Command (CINCUSSPACECOM) receiving the responsibility to be the lead CINC for CNA, the limited role by the Marine Corps is correct. However, with the expanding capabilities of potential adversaries (to be seen in chapter three), the Marine Corps should maintain close liaison ties with SPACECOM in CNA matters. This thesis tentatively recommends that “computer network attack” be modified to “computer network attack liaison.” Such liaison will be required to conduct offensive IO in the future, and such a liaison capability can prove valuable in providing a “reach back” capability to SPACECOM during MAGTF offensive operations in an unformed or developing operational environment.

The elements of offensive IO as listed in Joint Publication 3-13 include “Special Information Operations” (SIO), whereas the Marine Corps Concept Paper does not. SIO are defined as “Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the

United States, require a special review and approval process” (The Joint Chiefs of Staff 1998, GL-10). While this definition is intentionally vague, the MAGTF may be required to play a supporting role in such operations. Therefore, this thesis tentatively recommends that “support to SIO” be added to the elements of offensive IO. This serves as a reminder to MAGTF planners to conduct the appropriate planning and wargaming for supporting this element of offensive IO.

This chapter has answered the first subordinate question, which is: What is IO? The chapter also defined C2W and IW. The question: What are the elements of IO in accordance with the Marine Corps concept paper? was also answered. A tertiary question that was tentatively answered was: Should elements be added or subtracted in accordance with joint and other service doctrine? Two tentative recommendations were made, and will be discussed in greater detail in chapters four and five.

CHAPTER THREE

THREAT ANALYSIS

Introduction

The purpose of this chapter is to answer the subordinate question: What are the existing and emerging threats to the MAGTF's ability to conduct offensive operations in the future? Specifically, threats that can endanger the ability of a MAGTF to conduct offensive operations in a littoral environment, during an unformed or developing operational environment, are identified. Additionally, five tertiary questions are answered:

1. What threats can cause significant damage to a MAGTF during the preassault phase of an operation in a littoral region?
2. What threats can cause significant damage to a MAGTF during the assault phase of an operation in a littoral region?
3. What threats can cause significant damage to a MAGTF during the post assault phase of an operation in a littoral region?
4. What threats can cause significant disruption of MAGTF command and control in a littoral region?
5. What threats can cause catastrophic human casualties to a MAGTF in a littoral region?

As stated earlier, limitations to this research include:

1. The inability of researchers and writers to keep up with the rapid pace of the development of IO threats.

2. The inability to determine IO threats; because of their latent nature, they may only be discovered once their action is complete.
3. The plethora of threats in existence, both in form and actor.

In an uncertain world, future conflict is certain. Despite being the world's dominant power, U.S. superiority did not forestall ethnic war in the Balkans, nor did it prevent India and Pakistan from becoming nuclear powers (INSS 1999, 56). Where there is conflict, there will probably be a MAGTF.

The Marine Corps Intelligence Activity's *Midrange Threat Estimate 1997-2007: Finding Order in Chaos* accurately and briefly states that the Marine Corps must be prepared to fight large wars; to fight small wars; to respond to humanitarian emergencies; and to train and lend presence; whenever the needs of the nation direct (MCIA 1997, 41).

"Large wars" refer to the high- and mid-intensity conflicts that occur, the most recent involving significant Marine forces being Operation Desert Storm in 1991. "Small wars" have a long history in the Marine Corps. They include peace operations, counterinsurgencies, and a wide range of other military operations other than war (MOOTW). Responding to humanitarian emergencies can take place both internationally, such as disaster relief efforts in Operation Sea Angel in Bangladesh in 1991; and domestically, such as relief efforts in the wake of devastating hurricanes along the southeastern coast during the 1990s. "Training and lending presence" can occur with the MEUs deployed throughout the world, by mobile training teams (MTTs) teaching specific skills, or Marine Corps participation in North Atlantic Treaty Organization (NATO) exercises, overseas joint exercises, port calls and other activities.

Unformed and Developing Operational Environment

The “unformed” or “developing” operational environment where the MAGTF will find itself can be considered an “immature” or “emerging” environment. The unformed operational environment is characterized by an environment consisting of a crisis situation in which the objective, interoperability, and alliances and agreements may not exist or are unclear. The MAGTF will often provide the United States’ forward presence in this environment. The developing operational environment describes an environment in which the objective, interoperability, and alliances and agreements have been partially developed or clarified. Figure 2, from FM 100-7 *Decisive Force: The Army in Theater Operations*, shows the “unformed” or “developing” operational environments in relation to other operational environments.

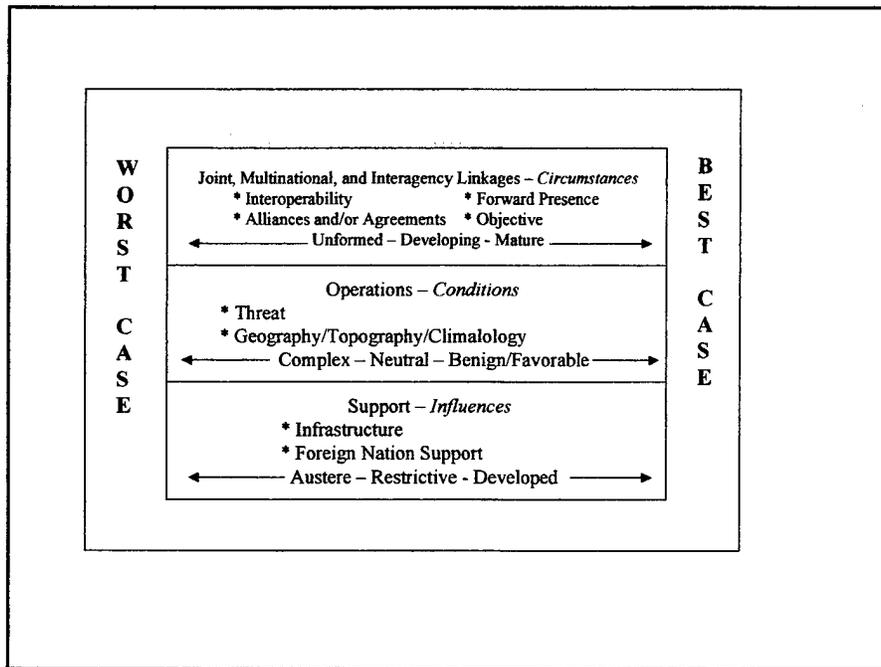


Figure 2. Operational Environments. Headquarters, Department of the Army, Field Manual 100-7, *Decisive Force: The Army in Theater Operations*. Washington, DC: U.S. Government Printing Office, May 1995, 2-28.

The Littoral Environment

A deployed MAGTF will usually execute the tasks listed above in an expeditionary environment. MCIAs defines the Marine Corps' expeditionary environment as the littoral region of the world. This region can best be described by three events: disasters, disruptions and disputes. These three events often threaten the national interests of the United States (MCIAs 1997, 1).

The most likely location of disasters, disruptions and disputes is at population centers. In 1997, 60 percent of the world's population lived within 100 kilometers of the ocean, 70 percent within 200 miles of the coast. The littorals control most of the productive land and seas in the world. Even though world trade moves largely by the oceans, the countries of the littoral regions control the chokepoints of the sea lines of communications (MCIAs 1997, 1).

Disasters can be natural or manmade (MCIAs 1997, 1). The increased populations of the littoral regions compound the effects of these disasters. The deployed MAGTF has been, and will continue to be, tasked to respond to these crises to alleviate human suffering. During these humanitarian assistance operations, typical threats to a MAGTF include disease, terrorism, and civil unrest. The vast majority of these typical threats can be countered by proper force protection.

Countries are vulnerable to disruption from below, within, and from above the state. Disruption from below the state include factionalism and demographics, which include urbanization, disease, and the "youth bulge," the phenomena of rapid population growth which tends to destabilize a state in which an overly large percentage of the population is unproductive because of young age, and is more prone to adopt radical

solutions to problems. Disruption from within the state includes state failures where the central state authority collapses or reaches near collapse. These forms of disruption can include revolutionary wars and insurgencies, ethnic conflicts, genocidal acts, collapse of state authority, the transition towards autocratic rule (to include *coup d'etat*), or turmoil associated with an uncertain succession of state leadership. Disruption from above the state includes the pressures and influences of alliances and international cooperation (including trade agreements); and transnational threats such as terrorism, proliferation, international drug trafficking, and international organized crime (MCIA 1997, 2-6).

Countries will continue to compete for power, prestige and control of resources. National cohesion will influence power; forces at work include internal national politics, and the building of new countries, often at the expense of old countries. The economic rivalries between countries are a source of potential conflict as well. Future demographic growth is forecast in the areas least able to support an increased population in terms of resources (food, water, shelter, raw materials, energy sources). This discrepancy will lead to population migration, internal strife, and interstate conflict (MCIA 1997, 6-8). This is reiterated in *Strategic Assessment 1999: Priorities for a Turbulent World* by the Institute for National Strategic Studies (INSS) of the National Defense University:

the growing chasm between the democratic core and the "have nots" portends a greater number of states and groups that see themselves excluded from the benefits of globalization. They have little stake in preserving international norms. Such states, as well as disenfranchised transnational organizations, are likely to join existing rouge states. (INSS 1999, 220)

Threat Analysis

Evaluation of threats to the MAGTF's ability to conduct offensive operations are based on the two following sets of threat identification and analysis criteria:

Force and time based set of criteria. (Subsets include threats to a MAGTF while underway; threats to a MAGTF inside the littoral battlespace, to include the preassault and assault phases of an amphibious operation; and threats to a MAGTF ashore, to include the assault and post assault phases.) MCIAs developed this set of criteria in their Midrange Threat Analysis.

Threats as defined by the severity of their potential consequences. This set of criteria was developed by Richard O. Hundley and Robert H. Anderson in their essay "Emerging Challenge: Security and Safety in Cyberspace" part of *In Athena's Camp, Preparing for Conflict in the Information Age* by John Arquilla and David Ronfeldt. Both sets of criteria will be explained in detail.

Littoral and expeditionary threats contained in the expeditionary environment: In the *Marine Corps Mid-Range Threat Estimate 1995-2005*, the MCIAs describe what type of conflict the Marine Corps must be prepared to fight and win, with what the future opponent may be equipped, and where the Marine Corps may be called upon to fight (MCIAs 1995, 37). In studying where the Marine Corps may fight, the MCIAs define the Marine Corps environment as an area that is littoral, and expeditionary, or subject to a high probability of instability and crisis (MCIAs 1995, 40). In the MCIAs threat estimate, countries that fit the set of criteria (littoral and expeditionary) are studied in greater detail, in terms of environmental factors, infrastructure and military capabilities.

Threats as defined by the severity of their potential consequences: In their article, "Emerging Challenge: Security and Safety in Cyberspace" Richard Hundley and Robert Anderson assign consequence categories to different threats. Although designed by the

authors for IO threats, I feel that these categories apply to other conventional and unconventional threats as well.

Hundley and Anderson use four categories to define the consequences of enemy attack. These categories are based on the degree of economic, human, or societal damage caused. From the least to the most consequential, they include:

1. Minor annoyance or inconvenience, which causes no important damage or loss, and is generally self-healing, with no significant recovery efforts being required.
2. Limited misfortune, which causes limited military, economic, human or societal damage, relative to the resources of the individuals, organizations, or societal elements involved, and for which the recovery is straightforward, with the recovery efforts being well within the recuperative resources of those affected individuals, organizations, or societal elements.
3. Major or widespread loss, which causes significant military, economic, human or societal damage, relative to the resources of those involved, and which may affect, or threaten to affect, a major portion of society, and for which recovery is possible but difficult, and strains the recuperative resources of the affected individuals, organizations, or societal elements.
4. Major disaster, which causes great damage or loss to affected individuals or organizations, and for which recovery is extremely difficult, if not impossible, and puts an enormous, if not overwhelming, load on the recuperative resources of those affected (Hundley & Anderson 1997, 232-233). (The author added “military” to the consequence categories listed above.)

Threats to the MAGTF

Regardless of the mission, threats to a MAGTF will be increasingly lethal. This will be particularly true in the littoral environment, where the range fans for sea-based, land-based and aerial weapons overlap. Additionally, future threats will have U.S. and other advanced country exports in their arsenals (MCIA 1997, 20). Since the threats against a MAGTF are becoming more diverse in actor and capability, the following delimitations are made to focus the threat analysis:

1. Only state actors and failed states are considered, terrorists and other nonstate actors are the subject of further research.
2. Antiship weapons, while extremely dangerous, are outside the scope of this research and are not considered. These weapons include antiship missiles, naval mines, fast attack coastal craft and diesel submarines. A U.S. Navy Officer would best research these weapons.
3. Nautical menaces and sources of instability such as pirates and narco-traffickers, while a growing concern, are not considered a significant threat to the ability of the MAGTF to conduct offensive operations and are not considered.

The first goal of a future potential or actual adversary will be to determine that a naval force is being assembled and is moving in his direction (MCIA 1997, 21). The increase of technology and communications makes the ability to watch the departure of a naval force from its homeport increasingly easy. These assets, coupled with even a primitive human intelligence network, make the departure of a naval force a hard thing to hide.

One of the advantages of a naval force is its ability to move significant distances while underway. OPSEC is improved, and the location of a naval force is harder to find. However, technology allows an increasingly larger number of countries access to satellite imagery. Even the poorest country can buy commercially available satellite imagery on demand. Long-range aircraft and increased electronic sensors make the ability to "hide" a naval force for extended periods harder, especially in littoral regions.

Once a naval force arrives at a littoral region, many countries will be able to bring significant, modern weapons to bear against the embarked MAGTF. The primary defense of the littoral will be in the air and the sea (MCIA 1997, 25). A partial list of these threats, by technology, that threaten the MAGTF during these phases of an operation (preassault, assault) include attack aircraft, antiair missiles, theater ballistic missiles (TBMs), coastal defense missiles/artillery, IO and weapons of mass destruction (WMD).

The technologies listed above can cause significant damage to a MAGTF and have the capability of cause catastrophic human casualties. Additionally, many of these technologies pose a threat to the MAGTF's shipping during the operation ashore. If these threats remain latent, they can pose a post assault threat to the MAGTF.

During the assault phase, several of the technological threats listed above can interfere with the MAGTF's operation. Attack aircraft can sortie against amphibious shipping, landing craft and units. Antiair missiles can be used against Marine aviation, hindering its use in the close air support (CAS) and assault support roles. Coastal defense missiles and artillery can target amphibious shipping, and interdict the surface ship-to-objective movement. Theater ballistic missiles (with or without WMD as warheads), can

target amphibious shipping and units ashore. Many of these threat technologies are capable of causing catastrophic human casualties to a MAGTF.

Once a MAGTF has landed ashore, adversaries will move forces to meet the perceived threat. The most significant threat to the MAGTF ashore will be posed by the armored and artillery elements of an enemy reaction force (MCIA 1997, 33). These forces will include main battle tanks, armored personnel carriers, infantry fighting vehicles, and light armored fighting vehicles. The proliferation of these weapons systems is immense. As an example, more than sixty families of light armored vehicles are in service around the world (MCIA 1997, 35). With the relative small amounts of organic armor and antiarmor systems, MAGTFs will rely on supporting arms to counter the armored threat. These same supporting arms will be used to neutralize the artillery within the enemy's reaction force.

Ultimately in the assault phase of an operation, the MAGTF ashore will have to engage the enemy by fire and close combat. The enemy may have access to new technologies in tactical target acquisition, night vision devices, antiarmor weapons, electro-optic countermeasures, mortars and small arms (MCIA 1997, 37).

Several threats can cause significant disruption of MAGTF command and control in a littoral region. These include many of the technologies listed above, such as IO and WMD. In particular, the proliferation of IO doctrine and technologies pose a significant risk to the command and control of a MAGTF. Of note are advances by Russia and China in this field. The MAGTF, in coordination with joint and service assets, must conduct defensive IO to counter these threats.

Table 5 summarizes the threats to the MAGTF's ability to conduct offensive operations in the future in matrix format.

Table 5.

Threats to a MAGTF, Matrixed.

Threat	M CIA (transit)	M CIA (preassault)	M CIA (assault)	M CIA (post assault)	Hundley & Anderson (minor)	Hundley & Anderson (limited)	Hundley & Anderson (major loss)	Hundley & Anderson (major disaster)
Sensors			X	X		X		
HUMINT	X		X	X		X		
Patrol aircraft	X	X	X			X		
Satellite imagery	X	X	X	X			X	
Attack aircraft		X	X	X			X	
Antiair missiles		X	X	X			X	
Coastal defense missiles/artillery		X	X				X	
WMD		X	X	X				X
IO	X	X	X	X				X
Enemy reaction force			X	X				X
Small arms technology		X	X	X			X	

The remainder of this thesis will focus on the MCIA force and time based set of criteria, threats to a MAGTF inside the littoral battlespace and threats to a MAGTF ashore; and Hundley and Anderson's major or widespread and major disaster categories.

CHAPTER FOUR

HISTORICAL EXAMPLES OF INFORMATION OPERATIONS

One assertion made at the start of this research was that although IO is a relatively new concept, warriors have long since been using the elements of IO to gain an advantage on the battlefield. Based on this assertion, the assumption is made that history will provide examples from which trends can be seen and doctrinal principles of offensive IO can be found for use by the MAGTF commander and staff of a deployed MAGTF in a littoral region with an unformed or developing operational environment. Under this assumption, this chapter conducts the historical analysis of examples in the search of doctrinal principles.

This chapter will answer the following subordinate question: Based on historical examples, what are general trends of IO that can generate proposed doctrinal principles of offensive IO for use by the MAGTF? Additionally, four tertiary questions are answered in this chapter and chapter five:

1. Based on historical examples, what are these proposed doctrinal principles?
2. Are these proposed doctrinal principles still relevant?
3. Are the doctrinal principles of IO shown by the selected historical examples feasible for use by a future MAGTF?
4. Will the doctrinal principles of IO shown by the selected historical examples add to the combat power of the MAGTF? If so, how?

To review, the criteria for selection of the historical examples contained in this chapter include the following:

1. The historical example was an operation that occurred in a littoral environment.
2. The historical example took place during or after World War II.
3. The historical example is a forerunner of what today would be considered an element of offensive IO.
4. The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future.
5. Two examples per element of offensive IO were used.

The analysis is based on historical examples chosen for the following reasons:

1. The doctrinal principles shown by these historical examples are still relevant. They have not been overcome by technology. They are useful against present and emerging threats.
2. The doctrinal principles shown by these historical examples are feasible for use by a MAGTF.
3. The doctrinal principles shown by these historical examples add to the combat power of the MAGTF.

To remain within the scope of this thesis, historical examples are limited to two examples per element of offensive IO. A case study of Operation Overlord will be used for the second example of each element of offensive IO, with the exception of the technologically new element of Computer Network Attack. Other examples may be referenced within a study, and other historical examples are listed for most elements. This provides a departure point for further research. It is hoped that follow-on researchers can use this information to further the study of IO within the Marine Corps. table 6 shows a matrix outline of the historical examples included in this chapter. (Other

relevant historical examples in studying the elements of offensive IO and their potential uses by the MAGTF can be found in appendix B.)

Table 6.

Historical Examples for Each Element of Offensive IO.

Offensive Element of IO	Example 1	Example 2
PSYOP	Faylaka Island	Operation Overlord Case Study
Deception	Operation Pastel	
OPSEC	Navajo Code Talkers	
Physical Destruction	Operation Just Cause	
EW	Operation El Dorado Canyon	
SIO Support	Yamamoto shootdown	
CNA Liaison	E-Commerce Attack	N/A

Psychological Operations

Example One: Psychological Operations against Iraqi Soldiers on Faylaka Island.

The psychological operations conducted against Iraqi soldiers on Faylaka Island during Operation Desert Storm are an excellent example of PSYOP in support of MAGTF operations. PSYOP is defined as “Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator’s objectives” (The Joint Chiefs of Staff 1998, GL-9).

This operation took place on Faylaka Island, which is found in Kuwait Bay of the Persian Gulf. It took place during Operation Desert Storm on 27 February 1991.

This operation employed PSYOP, which set the conditions for an unopposed amphibious landing.

The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future. An operation such as this could be carried out by a MAGTF afloat in the early stages of a crisis to begin the weakening of an adversary's morale. It could also be used as a supporting operation during the assault phase of a larger operation, as was seen at Faylaka Island, or during the post assault phase of an amphibious operation, as outlying remnants of the adversary's force are being cleared.

The Fourth Marine Expeditionary Brigade (MEB) was aboard amphibious shipping for Operation Desert Shield and during the first hours of Operation Desert Storm. On 29 January 1991, the 13th Marine Expeditionary Unit (Special Operations Capable) [MEU (SOC)] raided Umm Al-Maradim Island off the Kuwaiti coast. This was followed by amphibious feints to support the ground offensive from 20-26 February. These feints were aimed at Faylaka Island, the Ash Shuaybah port facility and Bubiyan Island (Summers 1995, 59). These operations distracted Iraqi attention, and continued to fix Iraqi forces along the Kuwaiti coast. The presence of Marine forces off the coast fixed four Iraqi divisions that were in defensive positions along the coast, plus two Iraqi armored divisions that were held in reserve. More than half of the Iraqi's 1,100 artillery pieces were pointed toward the sea (Summers 1995, 60).

Initial intelligence placed a 2,500 man Iraqi brigade on Faylaka Island (Department of Defense 1992, 217). An amphibious assault was scheduled for 28 February to seize the island. On 27 February, attached to Fifth MEB, Major Tabor Trischler and Specialist Jason Wells of the 9th PSYOP Battalion, with the aid of an interpreter, flew near the island in a Marine UH-1N helicopter equipped with a 2,700-watt loudspeaker system (Adolph 1992, 19). The PSYOP soldiers told the Iraqis to surrender the next day at the base of a nearby radio tower. The next day, 1,405 Iraqi soldiers, to include one general officer, waited in formation at the radio tower. Arriving Marine forces did not fire a single shot (Headquarters, Department of the Army 1996, 1-13). PSYOP, in conjunction with demoralizing physical attacks, led to this victory.

This incident was one of several during this time of Operation Desert Shield/Storm. The 101st Air Assault Division conducted a similar PSYOP with comparable results. The 490 Iraqi soldiers were compelled to surrender from an underground bunker (U.S. Army Special Operations Command n.d., 390).

In the Kuwaiti Theater of Operations (KTO), conditions were set for PSYOP to be effective, such as the use of EW and physical attack. This in turn resulted in PSYOP being a valuable combat multiplier. After being the target of days of bombing, shelling and psychological operations, many Iraqis were willing to surrender throughout the KTO. This is especially true because of the breakdown of Iraqi command and control, and the interdiction of their lines of communications. Many Iraqis were shell shocked and hungry by the start of the coalition ground offensive. In leveraging the use of PSYOP against the Iraqi soldiers on Faylaka Island, the presence of large numbers of embarked Marines in Kuwait Bay and their recent raids and feints reinforced the mood of

hopelessness among the Iraqis for their situation. The employment of PSYOP alleviated the need for a full assault against Faylaka Island and saved both Iraqi and American lives.

As shown in table 7, the combined use of several elements of offensive IO have proven extremely effective, which validates the joint doctrinal principle of offensive IO that “Offensive IO requires the integration and coordination of various capabilities.”

Table 7.

Combined Use of the Elements of Offensive IO, Faylaka Island.

Element of Offensive IO	Example
PSYOP	UH-1N broadcasts message to Iraqis to surrender
Deception	Previous feints by Marine forces off the Kuwaiti coast *
OPSEC	Location, intentions and timing of Marine forces hidden by amphibious shipping
Physical Destruction	Surface raid against Umm Al-Maradim Island; use of Marine aviation assets; earlier attacks against Faylaka Island
EW	Jamming by Marine and coalition aircraft

* The presence of three amphibious ready groups (ARGs) off the coast of Kuwait cannot be underestimated for their deception value. As stated earlier, these operations forced the commitment of six Iraqi divisions and approximately 600 pieces of artillery. In comparing land forces, this is approximately a six-to-one ratio.

Example Two: Operation Overlord Case Study

Allied psychological operations conducted against German soldiers in Cherbourg in 1944 will be studied as an excellent example of PSYOP. This operation took place in the European Theater of Operations during World War II. It occurred less than a month after the 6 June 1944 D-Day for the Normandy invasion.

As with the use of PSYOP against Iraqi soldiers on Faylaka Island, the potential exists for an operation similar to Cherbourg to take place by a MAGTF in a littoral region with an unformed or developing operational environment today or in the future. An operation such as this could be carried out by a MAGTF afloat in the early stages of a crisis, as a supporting operation during the assault phase of a larger operation, or during the post assault phase of an amphibious operation as outlying remnants of the adversary's force are being cleared, as occurred at Cherbourg.

Cherbourg was a major port in western France. Cherbourg, along with the port at Le Havre, would be essential in the throughput of supplies to the Allied Army in France. The Germans would undoubtedly sabotage the port facilities at Cherbourg, but its early capture would allow for the quick repair of the damage.

Throughout June 1944, German forces in the Cherbourg area fought against the Allied invaders stubbornly. By 18 June, the remnants of five German divisions were holding the city. In particular, the city's main fortification, the Fort du Roule, was heavily defended. American soldiers of the 314th Infantry Regiment captured the upper battlements and defeated diehard resisters by dropping demolitions into the bastion's lower reaches. Shortly afterwards, the city's commander surrendered but, on orders from Hitler relayed by General Erwin Rommel, refused to instruct his troops to do the same (Hammond n.d., 36). At that point, "American psychological warfare officers turned the trick. Dropping surrender leaflets that emphasized dwindling food supplies within the city, they announced that all who came across should bring their mess kits" (Hammond n.d., 36). Additionally, early on 27 June 1944, a truck equipped with a public address system was driven close to the defenders. A clear statement of the situation, to include

news of the capture of the city's commander, was broadcast. An appeal was made for the surrender of the defenders. Several hundred enemy soldiers took advantage of the offer (VII Corps G-3 1944). That evening, twenty days after the offensive had begun, the Allies secured Cherbourg (Hammond n.d., 36).

Cherbourg's capture is just one of several examples of PSYOP being used in Operation Overlord. To illustrate the scale of PSYOP during the landings in France, during the night of 8-9 June 1944, one million leaflets were dropped on enemy held cities in the VII Corps zone of action. These leaflets instructed the enemy on how to surrender (VII Corps G-2 1994).

In an obvious expeditionary example of PSYOP at Normandy, the Second Mobile Radio Broadcast Company were greeted by VII Corps G-2 personnel at Utah Beach as the company came ashore! They were informed that a leaflet was required immediately to gain the surrender of a group of surrounded German soldiers. However, the large numbers of previously printed leaflets had not yet been brought across the English Channel. Knowing the local situation would change before they could be obtained, the company mimeographed a crude leaflet to meet the situation (U.S. Army Special Operations Command n.d., 99).

By March 1945, the Allies had captured more than 850,000 German EPWs on the Western Front of Europe. In May, Brigadier General B. M. Bryan stated before the U.S. House of Representatives Military Affairs Committee that "more than eighty percent of the [German EPWs] brought with them into camp the leaflets scattered by American Air Forces containing assurances that no prisoners of war were or would be mistreated" (U.S. Army Special Operations Command n.d., 155). One particular PSYOP leaflet, entitled

the *Passieschein*, was an extremely formal-appearing surrender document that appealed to the German soldier's desire for a dignified surrender. According to interviews conducted on 375 German EPWs by the 21st Army Group, 275 had seen the *Passieschein*. Of those captured, 185 EPWs claimed they trusted it completely. Another thirty-two EPWs trusted it for the most part, with only twenty-one EPWs being disbelievers and nineteen EPWs being doubters (U.S. Army Special Operations Command n.d., 131).

The use of PSYOP in Operation Overlord saved Allied lives and sped the capture of early objectives. PSYOP eliminated the need to completely reduce the defenses of Cherbourg. The repair of port facilities was expedited. Additionally, PSYOP reduced German morale and attrited their forces by prompting the surrender of many German soldiers.

Deception

Example One: Operation Pastel, Deception in the Invasion of Japan

The deception plans developed to shield the United States' planned landings on the home islands of Japan (the Olympic and Coronet landings), are studied as an early example of deception. Deception is defined as "those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests" (The Joint Chiefs of Staff 1998, GL-5).

Operation Pastel took place in support of the planned invasion of Kyushu and the Tokyo Plain in the Pacific Theater of Operations. It took place in 1945 and was scheduled to go into 1946. This operation was based on deception, but also included OPSEC, EW and PSYOP.

The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment today or in the future. In part, an operation such as this could be carried out by a MAGTF afloat in the early stages of a crisis to force a reaction by the adversary's forces, or as a supporting operation during the preassault phase of a larger amphibious operation. Amphibious deception is only limited by planners' imaginations!

The objective of Operation Pastel was to reduce enemy strength in the invasion areas of the Japanese home islands by misleading the Japanese regarding American intentions and capabilities. Pastel was designed to reduce expected high casualties and to guarantee success of Operations Olympic and Coronet (Vander Linde 1987, 88; and Huber 1988, 1-2). As planning was conducted and the invasion neared, it could no longer be hidden from the Japanese. However, strategic deception could buy time until it was too late for the Japanese to redeploy forces from the continent of Asia to the home islands (Skates 1994, 160).

Convincing the Japanese of the Pastel deception story was to be a delicate, highly orchestrated affair. Seemingly random pieces of information had to be subtly released so that the Japanese would pick them up but would not immediately recognize a pattern. Individually, the bits and pieces of information would not seem connected. Accumulated and analyzed by the enemy's intelligence experts, the information would point the Japanese toward the desired conclusions--first the China coast, then Shikoku (Skates 1994, 162).

Pastel planners could not have expected the Japanese to accept this misdirection literally and to believe that there would be attacks on south Korea and on Shikoku but

that Kyushu would be spared. However, by plainly indicating that Korea and Shikoku were to be the landing targets, the planners created an element of ambiguity in the Japanese analysis. As a result, the Japanese were obliged to keep their forces at least partially dispersed (Huber 1988, 42-43).

Initially, the Japanese estimate was generally accurate about American objectives for the invasion of Japan as far as force levels and timing. However, Japanese concerns about airborne assaults and landings on Shikoku were inaccurate. American planners played on these fears in the Operation Pastel by encouraging the Japanese to believe that large airborne operations were being prepared. They also planned the use of the floating reserve force of Operation Olympic in a feint against Shikoku (Skates 1994, 104).

The airborne threat would also be used for tactical deception. On the night before the scheduled Olympic amphibious assault, airborne diversions would be flown to support each of the three landings; targets were Japanese airfields that were located behind the landing beaches. Similar diversions would be launched on the second night against airfields further inland. The planners hoped to distract and confuse the Japanese and force them to hold forces in reserve in the interior of the island while assault forces landed (Skates 1994, 164).

Even though the Japanese correctly estimated the overall American intentions, they faced the fundamental dilemma of all defenders against an amphibious assault. The Japanese had to decide whether to attempt to repel the invasion force at the beach and attempt to drive them back into the sea, or to hold forces in reserve further inland and attempt to destroy the American beachhead with a violent and coordinated counterattack. Both of these strategies could fail. To conduct a beach defense meant that the Japanese

had to guess the landing sites and landing force strength correctly. Holding forces in reserve would require consolidating scattered forces, moving them as required, and committing them to conduct a coordinated counterattack. The German example at Normandy showed that Allied air power could seriously disrupt the movement of counterattack units (Skates 1994, 104).

In a monograph by Barton Whaley entitled "Strategem: Deception and Surprise in War," Whaley states that a deception plan should encompass many possible alternative operations. If only one obvious possibility is developed, surprise is forfeited and the enemy will be able to mass forces. If at least one additional alternative is developed, the enemy's effectiveness could be halved. Additional alternatives will work, but contribute at a diminishing rate. Whaley's "Theory of Strategem" illustrates both the extreme importance of Operation Pastel and the plan's sound doctrinal approach. Operation Pastel presented several legitimate alternatives to the Japanese. This forced them to keep many of their forces dispersed (Huber 1988, 41-42). Huber also states, "A good deception planner is like a playwright who carefully orchestrates many small elements of reality to give the impression of a larger, but fictitious, reality. In this capacity, the Pastel strategists were resourceful" (Huber 1988, 43). Overall, Operation Pastel was a fairly sound plan "from a theoretical point of view." It was an "outstanding product of the American deceptionists' art" (Huber 1988, 44-45).

Thomas B. Allen and Norman Polmar in Code-Name Downfall confirm Huber's praise:

To some degree the deceptions and rumors of landings were successful. By April 1945, U.S. intercepts of diplomatic communications indicated that both the German ambassador to Japan and the Japanese military attaché in Stockholm had

the same idea: Americans were planning to land in China. Early in June, Japanese intelligence officers in South China were getting reports of actions that seemed to be connected to anticipated Allied landings. (Allen and Polmar 1995, 150)

However, Allen and Polmar do concede that with the proposed Coronet landings still months away, the results of the beginnings of its supporting deception operation (Pastel II) are hard to judge (Allen and Polmar 1995, 150). They also feel that despite the best efforts of Pastel, the best way to pin down the nearly three million Japanese troops in Manchuria and China to keep them unavailable for homeland defense was to entice the Soviet Union into the war (Allen and Polmar 1995, 230). However, this does not reduce the effectiveness of Pastel at the operational level in spreading Japanese defenses laterally and in depth.

The best evidence of the effectiveness of Pastel is from the Japanese themselves. According to Japanese military maps archived by the Japanese Demobilization Bureau records, the Japanese did believe that Kyushu would eventually be invaded, and even identified all three landings areas, probably through their own version of what could be considered intelligence preparation of the battlefield (IPB). However, they incorrectly assumed two airborne landings, which were not planned in actuality. The results for Operation Cornet and Pastel II are identical! The Japanese identified the landing areas, but also erroneously templated two airborne landings by one or two divisions (Superintendent of Records 1966, 653, 661).

By hinting at the use of several possible landings and landing sites by an amphibious force, planners of Operation Pastel were able to force the Japanese to disperse their forces laterally. With the addition of airborne deception, Japanese forces would be dispersed in depth as well. This idea can be used today, especially with the

increased range capability of the amphibious triad, and may be a good answer to mobile reserve forces.

Again, as shown in table 8, the combined use of several elements of offensive IO have proven extremely effective, which validates the joint doctrinal principle of offensive IO that “Offensive IO requires the integration and coordination of various capabilities.”

Table 8.

Combined Use of the Elements of Offensive IO, Operation Pastel.

Element of Offensive IO	Example
PSYOP	PSYOP radio broadcasts were to be transmitted to the Shanghai coast by the U.S. Army Forces, Pacific Psychological Warfare Branch
Deception	Fictional amphibious landings and airborne operations, media deception (using the press to announce false troop movements), phony units created
OPSEC	Naval transmissions controlled so as not to reveal that a large force was at sea before actual landings
Physical Destruction	Far East Air Force to conduct bombing and strafing missions against the defenses of fictional landing beaches
EW	Transmissions of phony orders to phony units

Source: Huber, Thomas M. Dr. 1988. *Pastel: Deception in the Invasion of Japan*. Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, December 1988, 6, 7, 8, 10, 16.

Example Two: Operation Overlord Case Study

The deception plans developed in support of Operation Overlord are studied as an early example of deception. Many of these efforts fell under Operation Fortitude South and Operation Fortitude South II.

As with Operation Pastel, the deception operations that supported Operation Overlord are good examples of amphibious deception operations. The potential greatly exists for similar operations to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future.

Deception was to play a vital role in the Normandy landings. Operation Overlord is an excellent example of where the element of deception was considered and planned throughout the development of the operation. The Allies deceived the Germans as to where the landings would occur, who (units) would conduct the landings, when and how the landings would occur.

Several deception operations were conducted in support of Operation Overlord. The more prominent operations are listed in table 9.

According to General Dwight D. Eisenhower, Supreme Allied Commander of the Allied Expeditionary Force:

We thought that to the German High Command an assault upon the Pas-de-Calais would be the obvious operation for the Allies to undertake. Not only was this the shortest sea journey where the maximum air cover would be available, but a lodgment in the Pas-de-Calais would lead the Allies by the shortest road directly to the Ruhr and the heart of Germany. . . . Acting on the assumption that this would be the German estimate we did everything possible to confirm him in this belief. (Supreme Commander, Allied Expeditionary Force 1946, 13)

To mislead the Germans into believing that the Pas-de-Calais, rather than the Cotentin, would be the site of the landings, Allied planners created a mythical First Army Group. This phony unit had an order of battle larger than that of General Sir Bernard Law Montgomery's Twenty-first Army Group. The First Army Group was "based" near Dover, just across the Channel from the supposed target. Dummy installations and equipment for the First Army Group were deployed.

Table 9.

Deception Operations in Support of Operation Overlord.

Operation	Objective
<i>Fortitude North</i>	Contain enemy forces in Scandinavia *
<i>Fortitude South</i>	Threaten the Pas-de-Calais region
<i>Zeppelin</i>	Threaten the Balkans in several locations
<i>Ironside</i>	Threaten Bordeaux, France
<i>Vendetta</i>	Threaten southern France
<i>Ferdinand</i>	Threaten western Italy
<i>Graffham</i>	Diplomatic deception in support of Fortitude North
<i>Royal Flush</i>	Diplomatic deception to convince the Germans that the Allies would attack southern France and use facilities in Spain; attempt to exploit the expected change in attitude of neutral nations to the Allies cause after the successful invasion of the continent
<i>Copperhead</i>	Notional journey of General Montgomery to Algiers, lower German vigilance in northwest Europe immediately before the invasion was launched
<i>Quicksilver I-VI</i>	Subsidiary deception operations to Fortitude South
<i>Titanic I-IV</i>	Ancillary deception operation; dummy paratroop drops used during D-Day
<i>Taxable</i>	Ancillary deception operation; simulated major surface assault on Fecamp during D-Day
<i>Glimmer</i>	Ancillary deception operation; simulated major surface assault on Boulogne during D-Day

Sources: Cruickshank, Charles. *Deception in World War II*. Oxford: Oxford University Press, 1979, 96-97; and Haswell, Jock. 1979. *D-Day: Intelligence and Deception*. New York: Times Books, 140, 192.

* "The threat to Scandinavia from Scotland in 1994 – *Fortitude North* – retained German troops in Norway and Denmark which would otherwise have been available for the defence of France" (Cruickshank 1979, 219).

Eisenhower assigned Lieutenant General George S. Patton, Jr. to command the fictional First Army Group. Patton was the American general the Germans most respected and feared. Allied naval units conducted protracted maneuvers off the Channel coast near the location of the First Army Group. Parts of the First Army Group conducted extensive

radio communications to signal to enemy signals intelligence personnel that a major military organization was functioning (Hammond n.d., 14, 15).

Hammond correctly states that Patton's nonexistent First Army Group was not the only reason that German commanders failed to deduce the correct location of Operation Overlord's landing sites (Hammond n.d., 18). The staging of actual units to participate in the invasion was done so as to support the Fortitude deception plan. This effort received the attention of senior commanders, to include Eisenhower. On the matter of staging areas, Eisenhower states:

Without departing from the principle that the efficient mounting remained at all times the first consideration, we took every opportunity of concentrating units destined ultimately for the Normandy beachhead in the east and southeast rather than the southwest. In this way it was hoped that the enemy, by his observations based on aerial reconnaissance and radio interception, would conclude that the main assault would take place farther to the east than was in fact intended. (Supreme Commander, Allied Expeditionary Force 1946, 13)

The same amount of consideration was given to the staging of seaborne assets. Again, Eisenhower reports:

Shipping arrangements were made with the same end in view. Surplus shipping was directed to the Thames Estuary where an enormous concentration was already assembled in preparation for the invasion, while landing craft were moored at Dover, in the Thames, and at certain East Anglian ports . . . After the assault had gone in on 6 June we continued to maintain, for as long as possible, our concentrations in the southeast and our displays of real and dummy shipping, in the hope that the enemy would estimate that the Normandy beachhead was a diversionary assault and that the main and positive blow would fall on the Pas-de-Calais when the diversion had fulfilled its purpose. (Supreme Commander, Allied Expeditionary Force 1946, 13)

Thanks in part to Operation Fortitude, the timing of the Normandy landings took the Germans by surprise: tactically, operationally, and strategically. With the employment of three airborne divisions on the night before the D-Day landings, their

very presence they caused confusion on the German side. Reports began to surface in German headquarters all along the Atlantic Wall that Allied paratroopers were landing, but little information was available to commanders on the size and meaning of the attack. The Germans had to ask: "Was it a probe to test Germany's defenses, a diversion for a larger assault in the Pas-de-Calais, or the long-awaited invasion itself?" The Allies further added to the confusion by parachuting dummies wired with firecrackers far to the rear of German positions (Hammond n.d., 21). This action drew major enemy units away from the objective area, further dispersing German forces laterally and in depth.

The example of deception in use to support the Normandy landings further validates the joint doctrinal principle of offensive IO that "Offensive IO requires the integration and coordination of various capabilities." FM 100-6 *Information Operations*, in citing the Normandy example, states:

Deception worked hand in hand with OPSEC to keep the organization and location of the real Overlord cantonments, training sites, dumps, movements, and embarkations carefully hidden. Unbelievable effort was put into creating mock airfields and ports, phony ships, boats, planes, tanks, vehicles, and troop movements, both real and staged. (Headquarters, Department of the Army 1996, 3-4)

The results of the Normandy deception efforts are dramatic. According to William M. Hammond, in *Normandy. The U.S. Army Campaigns of World War II*:

Although American commanders doubted that their ruses would have much effect, their schemes succeeded far beyond expectations. The Germans became so convinced that the Pas-de-Calais would be the Allied target that they held to the fiction until long after the actual attack had begun. As a result, nineteen powerful enemy divisions, to include important *panzer* reserves, stood idle on the day of the invasion, awaiting an assault that never came, when their presence in Normandy might have told heavily against the Allied attack. (Hammond n.d., 16)

According to Eisenhower's report:

The German Fifteenth Army remained immobile in the Pas-de-Calais, contained until the latter part of July by what we now know from high-level interrogation was the threat of attack by our forces in the southeast of England. Not until 25 July did the first division of the Fifteenth Army advance westward in a belated and fruitless attempt to reinforce the crumbling Normandy front. (Supreme Commander, Allied Expeditionary Force 1946, 13)

Charles Cruickshank in *Deception in World War II* further reiterates

there can be no doubt whatsoever that Fortitude South was an outstanding achievement. The First United States Army Group, originally in the substance and later in the shadow, induced the Germans to make disastrously false dispositions in France, and it certainly made a major contribution to the success of the invasion of Europe. (Cruickshank 1979, 220)

Adolph Hitler and Field Marshal Gerd von Rundstedt, commander of *Oberbefehlshaber West*, remained reluctant to commit the reserves they held in Pas-de-Calais because of the threat Patton's ghost army posed (Hammond n.d., 32). When these reserves were committed, it was too late.

To summarize the effects of deception in support of Operation Overlord, one can turn to Lieutenant General Omar N Bradley, U.S. First Army Commander:

While the enemy's Seventh Army, overworked and understrength, struggled to pin us down in the beachhead during July and August, the German High Command declined to reinforce it with troops from the Pas-de-Calais. There for seven decisive weeks, the [German] Fifteenth Army waited for an invasion that never came, convinced beyond all reasonable doubt that Patton would lead the *main* Allied assault across that narrow neck of the Channel. Thus while von Kluge was being defeated in the Battle for France, fewer than 100 miles away the enemy immobilized 19 divisions and played directly into our hands on the biggest single hoax of the war. (Bradley 1951, 344)

Deception had done its job at Normandy--and beyond!

Operations Security

Example One: Navajo Code Talkers in World War II

The Navajo Code Talker Program used by the U.S. Marine Corps during the Pacific Theater of Operations is studied as an early example of Operational Security (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. (The Joint Chiefs of Staff 1998, GL-9)

The Navajo Code Talker Program was an OPSEC measure that occurred in a littoral environment. It was used throughout the Pacific Theater of Operations in World War II. This historical example is an early use of OPSEC and is a forerunner of what today would be considered an element of IO. It functioned in the same role as today's cryptologic capabilities.

The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future. The MAGTF will use cryptology and other forms of OPSEC in the future to prevent the enemy from learning of its pending actions. Perhaps such a human element will give added information assurance (IA).

The Marine Corps' Navajo Code Talker Program was established in September 1942. The program was the result of a recommendation made in February 1942 by Mr. Philip Johnston. Mr. Johnston was the son of a missionary to the Navajo tribe and was

fluent in their language. He believed that using Navajo as a code language in voice (radio and wire) transmission could guarantee communications security. Mr. Johnston's rationale for this belief was that Navajo is an unwritten language and completely unintelligible to anyone except those intimately familiar with the language. It is a rich, fluent language for which code words, in Navajo, could be devised for specialized military terms. One example was the use of the Navajo word for "turtle" to represent a tank (Headquarters Marine Corps, History and Museums Division 1998, 1).

The first twenty-nine Navajos of the Code Talker Program devised Navajo words for military terms that were not part of their language. Alternate terms were provided in the code for letters frequently repeated in the English language. To compound the difficulty of the program, all code talkers had to memorize both the primary and alternate code terms. While much of the basic material was printed for use in training, the utmost observance of security precautions prevented the use of any printed material in a combat situation (Headquarters Marine Corps, History and Museums Division 1998, 1).

The Navajo language permitted the code talkers to use words with great precision. Once in theater, it became necessary to revise and enhance the code during the war. The code talkers learned new words and phrases that had to be adapted to the code. They also learned new and better techniques for sending and receiving their messages. During combat, the Navajos were able to improvise, sending and receiving messages that included words that were not in the original code. By using the precise meanings of each Navajo word, in new combinations, and verbs that could be changed according to what he wanted to say, a code talker could create and understand messages using words not in the original code.

The Navajo code was constantly updated and revised as required. For additional security, on Peleliu, every code talker was given two code numbers. If he was captured and the Japanese asked him to send a message, he was to send the message with one of the code numbers inserted. This would inform his headquarters that the message was not legitimate (Bixler 1992, 42, 78, 80-81). The Navajo Code Talkers were used for ship-to-shore and air-to-ground communications, as well as communicating between ground units, to include supporting arms (Wheeler 1983, 229).

While the battles of Tarawa and Saipan ended too quickly for their use, Navajo code talkers were used in the battles for Guadalcanal, Tinian, Peleliu, Iwo Jima, and Okinawa. On Tinian, they were used with good effect. Some of the Japanese radio operators spoke excellent English and tried to send out the wrong commands, but they could not decipher the Navajo code and sabotage the communications of the assault force (Bixler 1992, 93). According to Major Howard M. Connor, Signal Officer for the Fifth Marine Division, during the first forty-eight hours on Iwo Jima, more than 800 messages were sent and received without an error. Six Navajo radio nets that were operating around the clock within the division accomplished this feat. In occupied Japan, all messages about the atomic bomb devastation of Nagasaki, as well as the conditions in certain gun factories, were relayed by Navajo code talkers to the United States. Navajo code talkers were also used to report on the postwar situation in North China (Bixler 1992, 79).

Using the code talkers did have one drawback. Other American personnel, not familiar with the code talkers and thinking they were hearing the Japanese language, sometimes tried to jam the nets used by the Navajos (Bixler 1992, 82).

Estimates place the total number of Navajos in the Code Talker Program between 375 and 420 Marines. At the outset, the entire Navajo Code Talker Program was highly classified. While undoubtedly intercepted, there is no indication that any message traffic in the Navajo language was ever deciphered by the enemy (Headquarters Marine Corps, History and Museums Division, 1998,1; and National Security Agency, National Cryptologic Museum 2000, 1). Its effectiveness remains unparalleled. The Navajo code was only declassified when sophisticated encryption methods became available (Bixler 1992, 99). The Navajo Code Talker Program was an outstanding OPSEC measure whose implementation undoubtedly saved the lives of many Marines throughout the Pacific Theater of Operations.

Example Two: Operation Overlord Case Study

There are several examples of OPSEC within the preparations and conduct of Operation Overlord. OPSEC measures such as the ones used in Operation Overlord can be used to support similar operations to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future.

Numerous OPSEC measures were introduced well before the actual landings on 6 June 1944. These measures were varied, but mutually supporting to each other and the Fortitude deception plans. As with the deception plans, the Allies attempted to protect information pertaining to where the landings would occur, who (units) would conduct the landings, when the landings would occur, and to some degree by what methods.

According to Eisenhower:

Every precaution was taken against leakage of our true operational intentions against Normandy. The highest degree of secrecy was maintained throughout all military establishments, both British and American, but additional broader

measures affecting the general public were necessary as D-day approached.
(Supreme Commander, Allied Expeditionary Force 1946, 13-14)

These measures included suspension of all civilian traffic between Britain and Ireland on 9 February, a visitor's ban on the coastal area where the assault was being mounted to a depth of ten miles on 1 April, restricting of diplomatic privileges of British diplomats by the British government from 17 April to 19 June, and, on 25 May, a ten-day delay on all American mail from England was imposed, and American personnel were denied trans-Atlantic telephone, cable, and radio facilities (Supreme Commander, Allied Expeditionary Force 1946, 13-14). These measures were very proactive.

Annex 6d to VII Corps Operations Plan Neptune, dated 23 March 1944, contains detailed measures to protect operations security before D-Day. This annex, one of many such annexes in tactical operations plans, contains security measures during planning and training for the invasion, through measures in movement to the embarkation point. It even contains measures in the event units returned from the embarkation point because of an operational delay in embarkation (VII Corps G-3 1944, 6-D-1 to 6-D-3). Again, these security measures were very proactive. They were enacted to allow for the secure environment necessary to conduct the deception as outlined in Operation Fortitude.

Overlord planners felt that the concentration of ships in the southern ports of England was bound to be detected by the Germans, giving them some indication that Overlord was about to be launched. To confuse the Germans in this respect, arrangements were made with the British Admiralty to have the large number of commercial ships destined for the Thames River as well as the ships to be used in later supply convoys to Allied forces on the Continent held in Scottish ports until the Overlord

was under way. This shipping was spread throughout the British Isles and was not confined to a single area. As was the case against Sicily, Allied planners did not believe that the growing preparations and the size of the forces could be entirely concealed from the Germans. They hoped, however, to confuse the enemy as to the time of the assault and the objective area(s) (Supreme Commander, Allied Expeditionary Force 1946, 9). According to Eisenhower, "In this we were to be successful for a variety of reasons." (Supreme Commander, Allied Expeditionary Force 1946, 9).

In operations that can be described as counterintelligence (CI) as well as OPSEC, by 1944 British counterintelligence agencies had identified and either turned or eliminated virtually every German agent assigned to their island (Hammond n.d., 18). As with the proactive security measures aimed at civilians and military personnel mentioned earlier, these CI actions allowed for the secure environment necessary for Operation Fortitude.

Even the names of the Normandy operation were safeguarded. To protect the date of the invasion from the Germans, Allied planners called it D-Day. This name carried no implications of any sort. "Neptune," was the code name they used in place of "Overlord" on planning documents after September 1943. It was similarly devoid of any connotation to the amphibious assault against Continental Europe (Hammond n.d., 15).

Technology to assist in the Normandy landings was safeguarded as well. The Allies constructed two secret artificial harbors, called "Mulberries." Once an initial lodgment was made on the French coast, these Mulberries would be towed from England and anchored off the invasion beaches. They would be protected by artificial breakwaters and would enable large ships to unload in deep water. The ships' cargos would be moved

from ship to shore by either landing craft or pontoon causeways. According to Larry H. Addington in *The Patterns of War Since the Eighteenth Century*, “Probably no more technological invention involved in the invasion surprised the Germans more, or did more to undermine their basic strategy, than the Mulberries” (Addington 1994, 234). Basic German strategy was to throw the invasion back into the sea (Addington 1994, 234). The ability of the Allies to move supplies to shore without the initial use of the harbors of France relied to a large extent on the Mulberries. This made the Allies’ lodgment quicker and stronger, negating any chance by the Germans to drive the Allies “back into the sea.”

As seen by several examples, the effective use of OPSEC was critical before and during the amphibious landings on Normandy. OPSEC denied information to the Germans so Allied planners could “fill in the blanks” with deception. Yet again, the combined use of the elements of offensive IO proved extremely effective.

Physical Destruction

Physical Destruction Missions of Operation Just Cause

The use of physical destruction against H-Hour targets during Operation Just Cause, the invasion of Panama, is studied as an example of physical destruction supporting IO objectives. Physical attack or destruction refers to the use of “hard kill” (kinetic) weapons against designated targets as an element of an integrated IO effort (The Joint Chiefs of Staff 1998, II-5).

Operation Just Cause took place throughout the country of Panama, but concentrated near Panama City and the Panama Canal Zone. It occurred in December 1989. In terms of IO, this operation centered on physical destruction, but also included

PSYOP, electronic warfare and deception. Additionally, the hunt and subsequent capture of General Manuel Noriega, Panama's leader, can be considered an SIO.

The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment in the future. Marine ground and air combat elements could be used in a similar fashion as the assault echelon of Operation Just Cause in conducting physical destruction missions against enemy command and control nodes in support of the MAGTF commander's IO plan and concept of operations.

In 1989, the deterioration of relations between the United States and Panama led to the invasion of that country, Operation Just Cause. This operation was conducted to achieve four basic objectives: (1) protect U.S. citizens, (2) secure the Panama Canal, (3) support democracy for the people of Panama, and (4) apprehend Panamanian dictator Manuel Noriega (Department of Army 1989, 3).

As determined by the Southern Command (SOUTHCOM) G-2, the threat was primarily infantry. The Panamanian Defense Force (PDF) manned thirteen military zones throughout the country. The Panamanian Air Force had thirty-eight fixed-wing aircraft and seventeen helicopters. The Panamanian Navy had twelve vessels and a company of naval infantry (Flanagan 1993, 41). Paramilitary organizations, called "Dignity Battalions," were also present and were taken into consideration during planning. The PDF had the capability of reinforcing its garrisons with troops from other parts of the country. This reinforcement capability included light armored vehicles. The PDF's tactical disposition and equipment densities make it a light, yet good, model to study in an attempt to effectively counter a reaction force supporting a littoral defense.

Lieutenant General Carl Stiner, Commander of Joint Task Force (JTF) South, developed a plan of attack that called for a number of simultaneous attacks at various locations around Panama. Five conventional and five unconventional warfare task forces were assigned these objectives (Cole 1995, 38). Table 10 shows these objectives (various sources add or delete objectives, the table is a compilation of several sources):

These H-Hour targets can be classified as four categories. The first category includes physical destruction targets that were the command and control of the Panamanian nation, as well as the PDF. The destruction or neutralization of these targets is considered physical destruction in support of IO. The second category is PDF troop concentrations and reinforcement capability. This was an attempt to prevent PDF interference with the operation, and their removal from combat as quickly and simultaneously as possible. The third category was Panamanian and U.S. infrastructure. These targets allowed for the unimpeded arrival of follow on forces. Finally, the fourth category was the areas that had concentrations of U.S. Citizens.

The results of Operation Just Cause are common knowledge. Most objectives were secured near their anticipated times. As can be seen in table 10, some of the objectives were attacked late. This is because of the delayed arrival of several units of the 82nd Airborne Division because icy conditions at Fort Bragg delayed their departure. However, the attack of over twenty objectives in a near simultaneous attack is an impressive feat.

Table 10.

Operation Just Cause H-Hour Targets.

Objective	Time of Attack (Local, approximate)	Reason
<i>La Comandancia</i>	0029	Main PDF Headquarters
<i>Torrijos International Airfield/Tocumen Military Airfield</i>	0124	Deny Panamanian use/prevent Noriega's escape/Air Port of Debarkation (APOD)/ PDF 2nd Company Headquarters
<i>Tinajitas Garrison</i>	1050	PDF 1st Company Headquarters
<i>Panama Viejo</i>	0658	PDF 12th Cavalry Squadron Headquarters
<i>Fort Cimarron</i>	0017	Battalion 2000 Headquarters
<i>Coco Solo</i>	0050	Panamanian Naval Infantry Company Headquarters
<i>Fort Espinar</i>	0100	PDF 8th Company Headquarters/garrison at north end of Panama Canal
<i>Madden Dam</i>	0055	Controls water level of the Panama Canal
<i>Cerro Tigre</i>	0100	Electrical distribution facility/logistics center/PDF infantry company
<i>Renacer Prison</i>	0057	Free 67 Panamanian political prisoners jailed after 3 October anti-Noriega coup
<i>Fort Amador</i>	0100	PDF 5th Company Headquarters
<i>Rio Hato</i>	0100	PDF 6th and 7th Company Headquarters
<i>Balboa Harbor</i>	0045	PDF patrol craft/Noriega's yachts
<i>Cerro Azul</i>	0051	Panamanian television tower (prevent Noriega from rallying his forces by television broadcast)
<i>Punta Paitilla Airport</i>	0105	Deny Panamanian use/deny drug cartel use/prevent Noriega's escape
<i>Vicinity Howard Air Force Base</i>	0045	Secure air port of debarkation (APOD)
<i>Bridge of Americas</i>	0045	Deny Panamanian use
<i>Pecora River Bridge</i>	0045	Deny its use by Battalion 2000
<i>Colon</i>	0115	Isolate town
<i>Panama Canal Locks</i>	0100	Control Panama Canal
<i>Arrijan Tank Farm</i>	0045	Secure fuel supply
<i>Vera Cruz Bridge</i>	0045	Deny Panamanian use
<i>Carcel Modelo Prison</i>	0047	Rescue Central Intelligence Agency (CIA) operative

Sources: Donnelly, Thomas, Margaret Roth, and Caleb Baker. *Operation Just Cause, The Storming of Panama*. New York: Lexington Books, 1991, 80, 84-86, 100, 116, 124, 132, 188, 195, 218, 221, 228, 239, 256, 282, 289, 337; Flanagan, Edward M. Jr. LtGen, USA. 1993. *Battle for Panama, Inside Operation Just Cause*. McLean, VA: Brassey's, 44; Headquarters, XVIII Airborne Corps. *870-5a Organizational History Files. XVIII Airborne Corps. 1989-90. Operation JUST CAUSE. Corps Historian's Notes. Notebook #1*, U.S. Army, XVIII Airborne Corps, Fort Bragg, NC, 1990.; McConnell, Malcolm. 1991. *Just Cause*. New York: St. Martin's Press, 133, 165, 214; and Cole, Robert H. 1995. *Operation Just Cause, The Planning and Execution of Joint Operations in Panama, February 1988--January 1990*. Washington DC: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, 37-42.

This feat is comparable to “swarming” as described by John Arquilla and David Ronfeldt in their article “Looking Ahead: Preparing for Information Age Conflict” (Arquilla and Ronfeldt 1997, 465-477). Arquilla and Ronfeldt state:

Swarming is achieved when the dispersed nodes of a network of small (and also perhaps some large) forces can converge on an enemy from multiple directions, through either fire or maneuver. The overall aim should be sustainable pulsing--swarm networks must be able to coalesce rapidly and stealthily on a target, then disperse and redisperse, immediately ready to recombine for a new pulse. (Arquilla and Ronfeldt 1997, 465)

Units deployed to Panama conducted the first half of Arquilla and Ronfeldt’s swarming scenario. Their methods of attack combined with the selection of the targets made the initial assault against Panama a successful swarm against an enemy, paralyzing his command and control, then neutralizing his forces. The second half of Arquilla and Ronfeldt’s swarming scenario, that of redispersal, was not conducted in total because it was unnecessary in this scenario. However, certain units did disperse for follow on missions.

In addition to swarming tactics, targeting in Operation Just Cause fit the Basic Five Rings Model, which portrays an enemy as a system, quite well. This model, developed by Colonel John A. Warden III, USAF, is shown in figure 3.

In Operation Just Cause, the use of physical attack and destruction to eliminate the enemy’s command and control, troop concentrations, and reinforcement capability was used with great effect. The near simultaneous attack for multiple targets ensured an overwhelming use of combat power against the entire PDF to paralyze its leaders and reduce its combat effectiveness as quick as possible. This prevented the possibility of a future guerilla war by PDF troops.

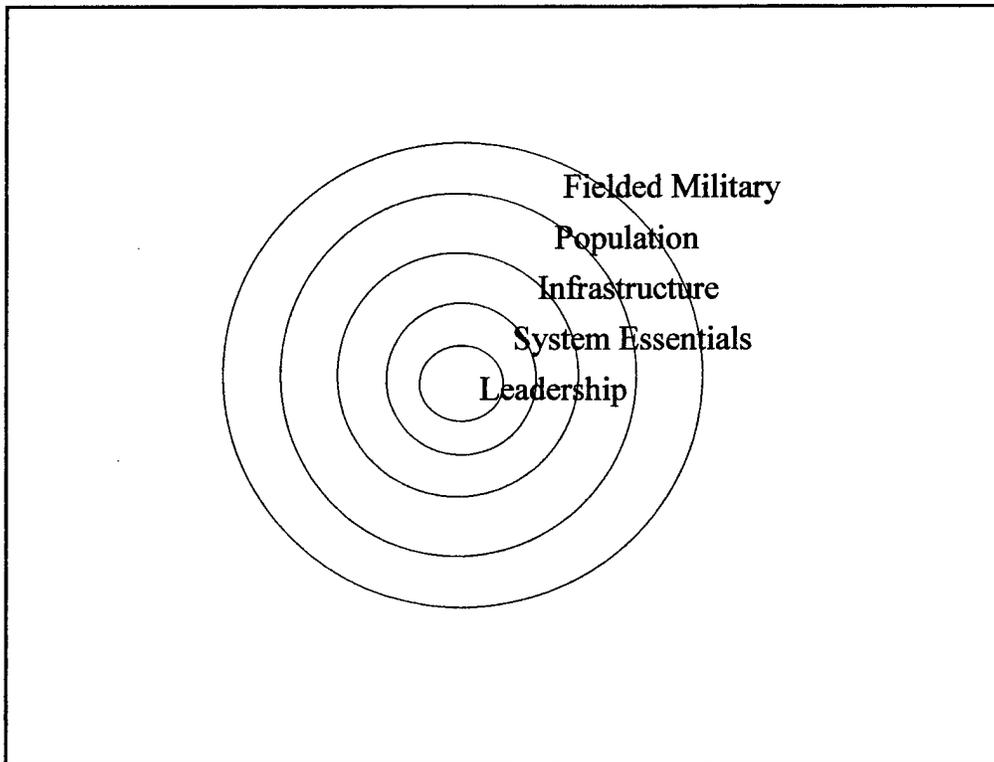


Figure 3. Basic Five Rings Model. Warden, John A., III. Colonel, USAF. "The Enemy as a System." *Airpower Journal*, Spring 1995, 44.

In this operation, the combined use of several elements of offensive IO proved effective, once again supporting the principle of offensive IO that "Offensive IO requires the integration and coordination of various capabilities." This combined use of the elements of offensive IO is shown in table 11.

Table 11.

Combined Use of the Elements of Offensive IO, Operation Just Cause.

Element of Offensive IO	Example
PSYOP	Increasing use of PSYOP to force remaining PDF units and personnel to surrender; support of the new, democratic government of Panama
Deception	"Sand Fleas" and other rehearsals
Physical Destruction	Swarming of over twenty targets to eliminate PDF command and control, troop concentrations, and reinforcement capability
EW	Jamming by EC-130 aircraft
SIO Support	Apprehension of Noriega

Example Two: Operation Overlord Case Study

As seen in the preceding example on Operation Just Cause, Operation Overlord made use of the element of physical destruction to support what would now be considered IO objectives. These types of physical destruction missions may be operations conducted in the future by a MAGTF in a littoral region with an unformed or developing, operational environment.

In preparation for and in support of the Normandy landings, physical destruction was used to degrade or eliminate the German's ability to gather intelligence and warning as to Allied intentions. Physical destruction was also used to support deception by attacking targets that were located in the Pas-de-Calais region, providing preassault targeting and destruction in support of Patton's mythical First Army Group. Finally, physical destruction supported the Normandy landings by interdicting the German mobile reaction force and preventing other reinforcements to Normandy.

Physical destruction prevented the Germans from knowing the details of Allied intentions. Before Operation Overlord was conducted, Allied warships had rendered German naval patrols in the English Channel ineffective. Additionally, Allied bombers had destroyed most of the German radar units that might have monitored air and naval traffic near the Normandy invasion beaches (Hammond n.d., 18).

In supporting Operation Fortitude South, physical destruction was used to support deception. A careful plan of aerial bombardment complemented the efforts of Allied planners to draw German attention away from Normandy and towards Pas-de-Calais. During the weeks preceding D-Day, Allied airmen dropped more bombs on the Pas-de-Calais than anywhere else in France (Hammond n.d., 14, 15).

Physical destruction supported the Normandy landings by preventing rapid German reinforcement. The Allies had air superiority in the vicinity of Normandy. Any German unit movements on roads and rail were susceptible to interdiction by Allied air attack. This forced the Germans to conduct night movements and cross-country movements, thereby dramatically slowing their rate of march. Additionally, members of the French resistance cut railroad tracks, sabotaged locomotives, and targeted supply trains in addition to the Allied aircraft that bombed roads, bridges and rail junctions to prevent the German reinforcement of the landing sites. To deceive the Germans further, these attacks occurred along the entire length of the French coast with the English Channel. By June, all rail routes across the Seine River north of Paris were closed. At this time the transportation system in France was at the "point of collapse" (Hammond n.d., 14).

In the week after D-Day, French resistance teams made 1,000 cuts on the rail lines of France; three weeks after D-Day the number was up to 2,000. After 7 June, not a single train crossed the area of Burgundy between Dijon, Besancon, Chalons and Lons-le-Saunier. This is the area through which ran all the main and secondary rail lines between the Rhone Valley and the Rhine. As an example of the results of the French resistance teams' work, as well as Allied air superiority, the German 11th Panzer Division took a week to get from Russia to the Rhine and three weeks to get across France to Caen. This is much longer than a division should take to cover this distance. In another example, one of the oldest and probably the best of the *panzer* divisions, "*Das Reich*," was ordered to Normandy from Toulouse. Normally a three-day trip, the division arrived fifteen days late (Casey 1988, 104).

These physical destruction missions played havoc with the Germans' concept of operations for the repulsion of the Allied invasion force. Field Marshal Gerd von Rundstedt, commander of *Oberbefehlshaber West*, placed great reliance on mechanized reserves that could respond quickly and flexibly to an Allied attack. He stationed a newly created armored command, *Panzer Group West*, near Paris. From that location, the force could move, as required, toward the site of an Allied assault in either the Pas-de-Calais or Normandy (Hammond n.d., 17). Physical destruction supported deception and severely complicated the movement and effectiveness of this mobile reserve.

Electronic Warfare (attack, support, protection)

Example One: Operation El Dorado Canyon

The use of EW during Operation El Dorado Canyon, the aerial bombing of Libya, is studied as an example of electronic warfare as a tool of IO in support of a conventional

operation. 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." The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support (The Joint Chiefs of Staff 1998, GL-6).

Electronic attack (EA) is "That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability." 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, or antiradiation weapons). Electronic protection (EP) is "That division of electronic warfare involving actions 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." Electronic warfare support (ES) is "That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing" (The Joint Chiefs of Staff 1998, GL-6).

Operation El Dorado Canyon was conducted on 14-15 April 1986. It was a retaliatory air strike against military targets in Libya. At that time, Libya was considered

a sponsor of international terrorism. Operation El Dorado Canyon is an example of the use of EW as a large component of an offensive operation. Jamming by Navy/Marine and Air Force aircraft was conducted, and antiradiation missiles and high-explosive bombs were employed against Libyan air defenses. The potential exists for MAGTF participation in an operation similar to El Dorado Canyon in the future.

Early in 1986, the leadership of the United States decided to take limited military actions against Libyan leader Colonel Mommar Gadhafi in response to Libyan sponsorship of international terrorism. During a four-day period in March 1986, a naval task force consisting of thirty ships, to include two carrier battle groups, conducted a freedom of navigation exercise in international waters adjacent to Libya's territorial waters. The exercise was a challenge to Gadhafi's claim to a substantial part of the Mediterranean Sea as Libyan territory. The Libyans responded by attacking the naval task force with patrol craft and surface-to-air missiles. All attacks were defeated at substantial loss to the Libyans (Parks 1986, 48).

On 5 April 1986, a bomb exploded in a Berlin discothèque that was frequented by U.S. military personnel. Approximately 200 people were injured, to include sixty-three American soldiers. One American soldier and one civilian were killed. Intercepted messages furnished what was described by the United States as evidence of Libyan involvement with the bombing, which was probably carried out by the Abu Nidal terrorist organization. On 14 April, Operation El Dorado Canyon was launched in retaliation (Metz 1987, 254).

On the night of 14-15 April, U.S. Naval and Air Force aircraft successfully attacked five separate targets in Tripoli and Benghazi (Parks 1986, 48). Eleven FB-111

bombers and four EF-111 electronic countermeasures aircraft were used, refueling several times in route. Twenty-four A-7E and F/A-18 strike aircraft and twelve A-6E attack aircraft participated from two nearby aircraft carriers (Venkus 1992, 145; and Metz 1987, 254-255). This force was supported near the objective area by F-14A Tomcat fighters for air defense, E-2C Hawkeye aircraft for command and control, EA-6B Prowler aircraft for EW, S-3 Vikings for antisubmarine warfare, K-A6 tankers for aerial refueling, and a SH-3 Sea King helicopters for search and rescue (Prunckun 1994, 77). Table 12 shows the targets, the force arrayed against them, and the results.

Table 12.

Results of Operation El Dorado Canyon.

Target	Aircraft Used	Results
Sidi Bilal (naval base used as a commando school)	3 X FB-111	Light damage
Aziziyah Barracks (Gadhafi's quarters at the time of attack)	3 X FB-111	Moderate damage
Tripoli Military Airfield	5 X FB-111	2 X I1-76 aircraft and some buildings destroyed
Benghazi (Jamahiriyah Barracks)	6 X A-6E	Barracks destroyed, warehouse damaged, 4 X MiG aircraft destroyed in shipping crates
Benina Airfield	6 X A-6E	4 X MiG-23 Flogger aircraft, 2 X Hip helicopters and two propeller planes destroyed; moderate damage

Sources: Parks, W. Hays. Colonel, USMCR. 1986. Crossing the Line. *Proceedings*. Annapolis, MD: Naval Institute Press, November, 48; and Prunckun, Henry W. Jr. 1994. OPERATION EL DORADO CANYON: A Military Solution to the Law Enforcement Problem of Terrorism--A Quantitative Analysis. Thesis submitted to University of South Australia, 80.

A sixth target category, not listed above, were the numerous Libyan surface-to-air missile sites in northern Libya. Twelve of these launchers were destroyed. In addition to the damage listed above, an estimated thirty-seven Libyans were killed and ninety-three injured (Prunckun 1994, 80). One FB-111 was lost, with its two-man crew killed.

As for the electronic warfare aspect of the mission, EF-111 and EA-6B aircraft provided EW against a sophisticated Libyan air defense network. Additionally, twelve Shrike and forty-eight HARM missiles were fired against Libyan air defenses. (The Shrike and HARM are antiradiation missiles.) The 500-pound "Snakeye" bombs and 750 pound cluster bombs were also used in an air defense suppression role (Prunckun 1994, 78). The aircraft that fired these missiles in the air defense suppression role accounted for 12 percent of the mission aircraft. Combined, the eighteen aircraft using EW in the EA and EP roles accounted for nearly the same percentage of total aircraft as the twenty-three main strike aircraft!

The results of Operation El Dorado Canyon were impressive. Five preplanned targets were struck in a moderately defended country, with minimal casualties. Operation El Dorado Canyon was an EW-intensive mission. Not using both EA and EP would have created numerous casualties, and have reduced the chance of mission success. As shown in table 13, the combined use of several elements of offensive IO proved extremely effective in Operation El Dorado Canyon.

Table 13.

Combined Use of the Elements of Offensive IO, Operation El Dorado Canyon.

Element of Offensive IO	Example
PSYOP	Notification of intent to retaliate against Libya
Deception	Previous naval action by naval forces off the Libyan coast
OPSEC	Secrecy involving the location, intentions and timing of units involved in the strike; Frequent readiness exercises at Royal Air Force Base Lakenheath disguised the departure of FB-111s on a combat mission
Physical Destruction	Air attacks against five targets (aerial swarming tactics)
SIO Support	Targeting of Gadhafi's quarters

The results of Operation El Dorado Canyon extended beyond their direct military implications. First, Gadhafi later instructed his operatives to reduce attacks on U.S. military targets but to look for easier U.S. targets. Second, the Soviet Union concluded that Libya's failed defense was a failure of men, not weapons. This led to the purge of some Libyan officers. Third, Syria publicly rejected the idea that Syria had any connection with terrorist activities. Fourth, the Soviet Union was in a weakened position. If they supported Gadhafi too much, they would drive him further away from conservative Arab support. If they did not support him, he might destroy his regime and the Soviet foothold in the Middle East. Fifth, Gadhafi's power within Libya was eroded. After the operation, he had to share power with four members of Libya's ruling Revolutionary Council. Additionally, from 1980 to 1986, ten attempts to remove Gadhafi by member of his military have occurred. These actions have taken place without U.S. intervention. Finally, Operation El Dorado Canyon prompted a more

concerted action against terrorism amongst the Western European nations (Goldstein 1996, 290-292).

Operation El Dorado Canyon is an example of a swarming aerial attack against fairly sophisticated air defenses located in a littoral environment. Such an attack may precede an amphibious landing, and can be modified from an air facilities and air defense-centered attack to a command and control and ground force-centered attack, much like Operation Just Cause.

Example Two: Operation Overlord Case Study

Much like the use of electronic warfare in Operation El Dorado Canyon, Operation Overlord effectively used EW against targets to support what would now be considered IO objectives. Much of this EW was used to support Operation Fortitude. According to FM 100-6 *Information Operations*, "A new era of deception was introduced--the electronic one" (Headquarters, Department of the Army 1996, 3-4).

By using physical destruction, German coastal defense radars were destroyed in a preconceived, highly calculated pattern. Overlord and Fortitude planners purposely left some intact near Pas-de-Calais; sixteen of the ninety-two German radar sites were deliberately spared (Breuer 1993, 175).

The night the Normandy landings were launched, the Allies began massively jamming German radars with chaff. However, the Allies purposely did not completely cover their targets. German radar operators had clear radar screens between the Allied jamming curtains. Within these clear zones, the Germans saw were two small fleets of small ships towing barges and blimps headed for Calais at eight knots, which is the speed of an amphibious fleet. Powerful electronic emitters, codenamed "Moonshine," received

the pulse of the German radars and sent it strongly back to the German receivers. For each iteration of this repeater jamming, it looked to the German operators as if a 10,000-ton ship had appeared. The small ships also had the recorded sounds of the amphibious assault at Salerno to play over speakers from ten miles out. German troops ashore could hear tapes of the sounds of the Allies getting into their landing craft for the run into the beach. Each Allied "fleet" appeared to be deployed over an area 256 square miles in size. One fleet was bound for Cap d'Antifer and fifty miles eastward was another steering for Boulogne (Breuer 1993, 176, 200). This operation confused the Germans for several hours. It played a major role in delaying German counteractions to the actual invasion at Normandy (Headquarters, Department of the Army 1996, 3-4).

Computer Network Attack Liaison

Example One: Computer Network Attack against Electronic Commerce

The Computer Network Attack (CNA) conducted against several well-known commercial internet sites is studied as an excellent, timely example of CNA. CNA is defined as "Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves" (The Joint Chiefs of Staff 1998, GL-5). *A Concept for Information Operations* states that the Marine Corps will play a limited role in CNA (Marine Corps Combat Development Command 1998, 4). In chapter two, this thesis tentatively recommended that "Computer Network Attack" be modified to "Computer Network Attack Liaison." This example will be studied as CNA, and analyzed as CNA Liaison towards the end of the analysis.

In studying CNA, the criteria of the littoral environment must be placed aside. CNA technology can strike targets through all regions of the world. The CNA incident

that serves as this thesis' example took place in February 2000. A Federal Bureau of Investigation (FBI) investigation is still ongoing. This example is an incident of CNA conducted by unknown perpetrator(s) against internet-based commerce.

The potential exists for a similar operation to take place by a MAGTF. An operation such as this conducted by national assets and coordinated by the MAGTF afloat in the early stages of a crisis could disrupt or destroy critical parts of an adversary's command and control system, weapons systems, or infrastructure. CNA such as described in this example could be conducted during all phases of an amphibious operation. Likely operational and tactical targets include command and control systems, sensors, antiship and antiair missile systems, guidance systems, tactical navigation systems, communications networks, and infrastructure that support the coastal defense and movement of the mobile reserve.

The history of CNA began in 1988, when the world saw the first well-publicized case of a computer virus. This self-replicating virus, known as the "internet worm," penetrated the computer system at the University of California at Berkeley. It then corrupted thousands of computers, totaling 10 percent of all computers connected to the internet. In response, a Computer Emergency Response Team (CERT) was created at Carnegie Mellon University, which was the first of many in a "growth industry." In 1993 the Carnegie Mellon CERT had their first large event as they put out a warning to network administrators that a band of intruders had stolen tens of thousands of internet passwords. When this CERT began in the late 1980s, they processed less than fifty events per year. Now they process thousands of events per year (Headquarters, Department of the Army 1996, 3-9; Fithen 2000, 1). Other cyberattacks include web-

specific attacks, where internet users accessing a web site receive information that operators of the site may not have intended to send; and IP spoofing, where attackers run a software tool that creates internet messages that appear to come from a computer trusted by the victim, not from the attacker (Cross 2000, 3-5). These are only a few of the diverse cyberattacks that currently exist.

In an unauthorized use, CNA is referred to as "cybercrime." This type of crime has increased through the years. In 1998, the Federal Bureau of Investigation (FBI) opened 547 computer-intrusion cases. In 1999, that number doubled to 1,154. According to FBI Director Louis Freeh, "In short, even though we have markedly improved our capabilities to fight cyber intrusions the problem is growing faster and we are falling further behind" (Reuters Newswire 16 February 2000).

On 8 October 1999, Army General Henry Shelton, chairman of the Joint Chiefs of Staff, acknowledged for the first time that the United States military used a form of computer warfare against Yugoslavia as part of NATO's air campaign during the spring of 1999. Shelton said the "systems" were offensive in nature. A defense official said later that Shelton was referring to a broad range of IO involving computers that might have included cyber-attacks on Yugoslavia's air defense network (Associated Press Newswire 8 October 1999). The precedent for military application has been set.

On Monday, 7 February 2000, "Yahoo!," a popular internet search engine, electronic mail (e-mail) service provider and news service was hit by an electronic attack that knocked the site offline for three hours. This attack was followed on Tuesday by attacks on Buy.com, eBay, Amazon.com, and CNN. On Wednesday, 9 February 2000,

E*Trade and ZDNet were attacked (Mack 2000, 1). All of these sites are news providers, online auctioneers and brokers, or electronic commerce (e-commerce) venues.

The attacks against these high-profile web sites were classified as “distributed denial of service” attacks. These attacks are conducted in the four steps shown in table 14.

Table 14.

Conduct of a Distributed Denial of Service Attack.

Step	Action
1	A computer attacker electronically breaks into a large number of unsecure computers. These computers are called “zombies.”
2	The attacker installs files on the “zombies.” These files remain dormant until called upon.
3	From a remote location, the attacker orders the “zombies” to send massive amounts of bogus data to a targeted web site.
4	The deluge of bogus data sent against the targeted network cripples it. The internet addresses on the forged data are “spoofed”, making the attacker difficult to track.
Result	Internet users trying to log on to the attacker site encounter the equivalent of a busy signal and are denied access.

Source: Koerner, Brendan I. 2000. The Web’s Bad Week. *U.S. News & World Report*. 21 February, 19-20.

During the cyberattack’s peak, Yahoo! received one gigabit of incoming data per second, this is more than most sites receive in a year. Greg Shipley of the security consulting firm Neohapsis states: “It’s like a bunch of small piranhas mowing down a large cow” (Koerner 2000, 19).

Unfortunately, for a distributed denial of service attack, conventional firewalls of intrusion detection systems are powerless to halt the massive information flow into the web site. Locating and disabling a single “zombie” is futile, given the large numbers of machines used by the attacker. The computer vandal that conducted this “three-day blitzkrieg” against these e-commerce sites employed what is considered a “relatively juvenile” intrusion technique. This electronic blitzkrieg showed the “inherent insecurity of America’s favorite technological marvel and the inability of both law enforcement and the private sector to guard their cyberturf” (Koerner 2000, 19). According to Christopher Klaus, chief technology officer of Internet Security Systems, “It’s definitely a wake-up call. . . . This is a serious underpinning of our economy. If it isn’t protected, it could be much more serious than just these bookstores going down” (Koerner 2000, 19).

Unfortunately, in a well-known case such as this, “The possibility of copycats is out there, as are other theories, with these piggyback incidents,” stated an FBI spokeswoman (Sniffen 2000, 1). At present, information released by the FBI indicates that some “zombies” have been identified. The FBI is pursuing leads, several of which are outside the borders of the United States. The attacker(s) is (are) still not known.

According to Katherine T. Fithen, Manager of the CERT Coordination Center at the Carnegie Mellon Institute, “only partial solutions” are available against distributed denial of service attacks. She states, “There is essentially nothing a site can do with currently available technology to prevent becoming a victim of, for example, a coordinated network flood” (Fithen 2000, 1).

As can be seen by this distributed denial of service cyberattack, relatively simple methods can be used to disable web sites. This attack also underscores the vulnerability of the internet, web sites, e-mail, computer hardware, and computer software.

A denial of service cyberattack, as well as other forms of CNA, have a military application. One only has to substitute the recent attacks against e-commerce for similar attacks against the mobile reserve of a MAGTF's adversary to visualize the military potential of CNA. The MAGTF must have the resident planning knowledge to integrate the combat multiplier of CNA into traditional amphibious operations.

Support to Special Information Operations

Example One: The Attack against Admiral Yamamoto, an Early Example of an SIO

The attack of Admiral Isoroku Yamamoto, commander-in-chief of the Japanese Combined Fleet, is studied as an early example of an SIO. SIO are defined as "Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process" (The Joint Chiefs of Staff 1998, GL-10).

This operation took place in 1943 in the Pacific Theater of Operations during World War II near Bougainville. A forerunner of what today would be considered an element of IO, this operation was based on a radio intercept (EW) and resembles what an SIO would look like today. It ended in the physical attack and destruction of the target. Deception was involved to make the attack look like a target of opportunity and not preplanned.

The potential exists for a similar operation to take place by a MAGTF in a littoral region with an unformed or developing operational environment today or in the future.

An operation such as this specific example could be carried out by an aviation combat element (ACE) of a MAGTF.

History provides us a great example of an SIO. In his book, *Attack on Yamamoto*, Carroll V. Glines states:

It is generally agreed among military historians that reading the secret messages of an enemy is the most important form of intelligence information that a nation can have. It is more accurate than information provided by spies and it has been shown to have great influence on a nation's strategy and politics in both war and peace. (Glines 1990, 13)

In the early hours of April 14, 1943, three U.S. naval radio intercept units intercepted a Japanese message. American intelligence had learned from intercepted and decoded radio messages the itinerary of Admiral Yamamoto. Yamamoto, the man who had masterminded the attack on Pearl Harbor, would depart Rabaul on the northern coast of New Guinea and arrive at an airfield on the southern tip of Bougainville on the morning of April 18, 1943 (Glines 1990, ix-x, 1, 30). This Japanese message was deciphered and translated in five hours during the evening of April 13-14, 1943. Cryptanalysts and translators in both Pearl Harbor and Washington, DC were involved, trading information (Davis 1969, 10-11, 14). This teamwork was a forerunner of the "reach back" capability that exists today.

Admiral Chester W. Nimitz, Commander-in-Chief, U.S. Pacific Fleet, was briefed soon after. He requested that U.S. forces intercept and destroy the enemy bomber that carried Yamamoto. According to Carroll V. Glines, debate exists whether the Secretary of the Navy Frank Knox or President Roosevelt were informed. There are no official White House records of this matter available (Glines 1990, ix-x, 2, 13). Burke Davis, author of the 1969 book *Get Yamamoto*, states that Roosevelt and Knox, as well as

General Henry H. Arnold, Chief of the Army Air Forces, were informed of the mission and gave their approval. Davis states that this information was deliberately omitted from official records (Davis 1969, 15-20). Edwin P. Hoyt, in his 1990 book *Yamamoto*, states that both Roosevelt and Knox, as well as the Chief of Naval Operations, Admiral King, knew of the attack. Hoyt states that Roosevelt gave the order to proceed with the attack (Hoyt 1990, 248). Despite this debate, it is safe to assume that enough senior officials knew and approved of the mission to classify it as a SIO.

This mission made use of an extremely sensitive capability, that of breaking Japanese naval codes. It also had an extremely important potential effect or impact in the Pacific Theater of Operations, by removing the enemy's most capable naval strategist. Because of the source of the intelligence, it also had a special review and approval process. All of these factors strengthen the characterization of this mission as an SIO. This is contrary to FM 100-6, *Information Operations*, which classifies this event as an example of physical destruction.

On the morning of April 18, 1943, a squadron of sixteen Lockheed P-38 fighters from Guadalcanal conducted the longest successful fighter intercept mission ever flown by American fighter planes to that date. Two enemy bombers were shot down and Admiral Yamamoto was killed (Glines 1990, ix-x, 1, 38). P-38s were used because of their superior range.

Aside from the Emperor, there was no one held in higher regard by the Japanese public than Yamamoto. His loss was a terrible blow to Japanese morale, and was later an extraordinary morale boost for the Americans in the Pacific. As stated by Glines, "The Japanese people were devastated by the loss of their beloved naval leader. His death was

a severe blow to national morale--a blow as cruel to their psyche as the Doolittle raid on Tokyo had been a year before" (Glines 1990, 1, 3, 124). Admiral Matome Ugaki, Yamamoto's Chief of Staff, confirms this by stating, "Even in death, dignity did not leave the great naval officer. To us, Isoroku Yamamoto virtually was a god" (Davis 1969, 197). Yamamoto's death temporarily reduced the effectiveness of Japanese command and control and temporarily hampered their war effort. One can argue that he was irreplaceable as a military strategist.

There are two lessons learned from the Yamamoto mission that are applicable today. One is the determination of when a target is worth risking the intelligence source for. Although the loss of Yamamoto was a tremendous blow to the Japanese, U.S. naval cryptographers were apprehensive from the start that the Japanese would realize that their communications were unsecure (Glines 1990, 119). This would cause the Japanese to change codes and possibly change communications means. This could end America's ability to eavesdrop on Japanese communications, an ability that led to the culmination of Japanese gains in the Pacific and a shift in momentum to the Allies. The second lesson learned was the importance of protecting intelligence sources. As stated by Glines, "The protection of a codebreaking capability is just as important as protecting the results of codebreaking." Every effort was made to make the intercept look "fortuitous." The attacking P-38s maintained radio silence. Their route was over water, far away from any Japanese bases. Finally, the results of their mission were a closely guarded secret for some time, and possible security leaks from the operation were quickly investigated and sealed (Glines 1990, 8, 23).

The Japanese accounted the Yamamoto shootdown to sheer coincidence. Even before the shootdown, Admiral Kusaka Jin'ichi [Joshima], commander-in-chief of the Southeast Area Fleet, had on two or three occasions the "uneasy feeling" that information was leaking to the United States through the deciphering of Japanese codes. The result of his inquiry to the Fourth Division of the Naval General Staff was that such deciphering was impossible. Admiral Ugaki himself stated, "How could they possibly break the Japanese codes?" It was not until after World War II ended that they found out the Yamamoto shootdown did occur because of the exploitation of such cryptologic intelligence (Agawa 1979, 369). The thought of Japanese code invincibility is confirmed by Admiral Ugaki, who writes in his diary in 1944 that the shootdown was "just a turn of fate" (Ugaki 1991, 350-351, 360). Only Hoyt disagrees with the level of security involved in the operation. He writes that an Australian new reporter on Guadalcanal broke the story upon his return to Australia, and the Japanese picked the news up from a newspaper in Argentina. However, senior Japanese officials did not believe the story (Hoyt 1990, 249). The vast majority of evidence strongly suggests that the intelligence source was properly protected in this example.

Once again, the combined use of several elements of offensive IO have proven extremely effective, which validates the joint doctrinal principle of offensive IO that "Offensive IO requires the integration and coordination of various capabilities." Table 15 shows the combined use of the elements of offensive IO in this operation.

Table 15.

Combined Use of the Elements of Offensive IO, The Attack against Admiral Yamamoto.

Element of Offensive IO	Example
PSYOP	Damage to Japanese morale
OPSEC	U.S. naval code breaking capability closely safeguarded; operation made to look like a random incident
Physical Destruction	P-38s conduct actual physical destruction
EW	U.S. Naval electronic collections capability

Glines states, “To term the Yamamoto mission as a special operation, it had the basic characteristics of “special ops”--speed, accuracy, and a linkage to technical intelligence systems and psychological operations” (Glines 1990, 164). Using the definition of SIO from Joint Publication 3-13, one can see that the Yamamoto mission was of a sensitive nature. The impact of Yamamoto’s death had strategic implications. Additionally, the information of Yamamoto’s movements was obtained by highly classified means. Finally, a special review and approval process was used, terminating with Admiral Nimitz, and possibly Secretary of the Navy Knox and/or President Roosevelt.

Because of their forward-deployed nature and inherent flexibility, MAGTFs must be able to support such SIOs in the future. The use of MAGTF aviation, electronic warfare, and other assets may be used to take advantage of any fleeting opportunities created by the United States’ control of information. Additionally, such an operation could be mounted against the leadership of an adversary’s military, and specifically the leadership of an enemy’s coastal defenses and/or mobile reserves.

Example Two: Operation Overlord Case Study

During the preparations of Operation Overlord, several deception plans were instituted that are termed “diplomatic deceptions” by Charles Cruickshank in *Deception in World War II*. Of these, one, Operation Royal Flush, is studied as an early example of what would now be classified as an SIO.

Operation Royal Flush was a deception plan to support the earlier overall deception effort against Germany, Operation Bodyguard. Operation Royal Flush supported earlier efforts to hint at an invasion against the southern coast of France, the Balkans, and Scandinavia. Allied planners believed that when neutral nations saw that the Allies had gained a secure foothold in France, the most important nations, Spain, Turkey and Sweden, would decide that they had little to fear from German reprisals. They might provide some discrete assistance to the Allies. In particular, transit facilities would be helpful (Cruickshank 1979, 138).

Spain was asked for facilities indicating an Allied invasion into southern France. Examples include the evacuation of casualties and the throughput of food. The British Ambassador to Spain, Sir Samuel Hoare, went to London to personally be briefed, a move which helped in the deception. The American Ambassador placed great importance on these requests, increasing the legitimacy of the deception (Cruickshank 1979, 139-142).

As these requests were being made to Spanish authorities, British and U.S. diplomats appeared at the port facilities of Barcelona, making what could be called a “leader’s reconnaissance” as to the availability of billeting and throughput capacity (Brown 1975, 612).

Spain later agreed to these requests, but only after military action had begun. The Spanish portion of Operation Royal Flush was complete in July 1994 when both British and American diplomats informed Spanish officials that the success of the Normandy landings made Spain's help unnecessary (Cruickshank 1979, 139-142).

The Germans received information of Spain's approval. This information, along with intelligence of the growing size of the French First Army in North Africa, the presence of the U.S. 91st Infantry Division (an assault-trained unit) in North Africa, and the presence of Allied reconnaissance ships and aircraft, Field Marshal Rundstedt decided to keep the entire Army of the Riviera in place, to include its *panzer* divisions (Brown 1975, 612-613).

Turkey was one key to containing German forces in the Balkans. However, diplomatic deception against Turkey, while planned, was not executed in support of the Normandy landings. This was largely because the British did not want to weaken their standing with regard to Turkey by asking for assistance. Therefore, economic pressure was continued against Turkey. The Germans believed that this was an attempt to force Turkey into the war on the Allied side. The Allies relied on these German beliefs to keep German forces in the Balkans and prevented their use on the Western Front (Cruickshank 1979, 142-143).

Diplomatic deception against Sweden to break their strict neutrality did not succeed. The Swedes did reduce their exports of iron ore and ball bearings to the Germans, and assured the Allies that any German invasion would be met with strong Swedish resistance. However, the Swedes would budge no more. In this instance, Operation Royal Flush was not effective (Cruickshank 1979, 143-144).

Operation Royal Flush meets the criteria to be categorized as an SIO. Since diplomatic services were involved, an operation of a sensitive nature existed. Operation Royal Flush could not only potentially tie down numerous German divisions, but could potentially turn a neutral nation into an ally. This meets the criteria of “potential effect or impact, security requirements, or risk to the national security of the United States (or her Allies).” Since Operation Royal Flush involved diplomats, a highly centralized, diplomatic approval process was used, meeting the requirement for a “special review and approval process.”

Because of their forward-deployed nature and inherent flexibility, MAGTFs may support SIOs in the realm of diplomatic deception in the future. The use of the MAGTF’s command element, as well as its mobile training team (MTT) capability and ability to conduct training exercises with the militaries of other nations, allows for one forum of supporting diplomatic deception.

CHAPTER FIVE

CONCLUSIONS AND RECOMMENDATIONS

The purpose of this thesis is to propose doctrinal principles for the employment of offensive IO that are more specific than current joint doctrine and are based on successful historical examples. These doctrinal principles are proposed in this chapter. They are specific to a littoral region with an unformed or developing, operational environment.

This chapter marks the completion of the interpretative phase of research, which was step four of this thesis' research process. Chapter five marks the application of data to the present and provides hypotheses for the future, which is step 5 of this thesis' research process.

This chapter also answers the questions: Will the doctrinal principles of IO shown by the selected historical examples add to the combat power of the MAGTF? If so, how? Additionally, the chapter determines the most necessary and useful elements of offensive IO for a MAGTF. It is expected that these elements vary in relation to the intensity of conflict. Additionally, this research identifies shortfalls in elements of offensive IO and makes recommendations on whether to research these areas further, allocate resources to counter the threats, or rely on other services for support.

All proposed doctrinal principles are informally compared to existing joint doctrine to ensure there is little, if any, duplication. Additionally, they are compared to the principles of OMFTS to ensure doctrinal consistency. Criteria used to determine the most necessary and/or useful elements are the principles of OMFTS, which were shown in table 2 of this thesis.

Conclusions: PSYOP

Three possible doctrinal principles are identified for the use of PSYOP in the context of this thesis. First, PSYOP should be considered in all potential operations; it is a proven combat multiplier. Second, PSYOP can be used to reduce the enemy's will to fight. It can reduce strongpoints and increase a MAGTF's operational tempo. Finally, PSYOP themes must be consistent with future JTF commanders and the geographic CINC's desires. Therefore, PSYOP planning should be proactive, fueled by continuous intelligence and guidance from higher headquarters. All three of these possible doctrinal principles are supported by the selected historical examples.

As is seen in the Faylaka Island example, the use of PSYOP the day before a scheduled amphibious assault allowed for the capture of the island's garrison without a shot being fired by amphibious forces. At Faylaka Island, the use of PSYOP took advantage of the isolated and demoralized situation of the Iraqi troops that were the subject of previous deceptions, EW and physical attack. The seizure of the island could have been accomplished with a smaller force. This shows the ability of PSYOP to be a combat multiplier. In conducting the Operation Overlord Case Study, an example of the use of PSYOP against German troops in Cherbourg closely mirrors the Faylaka Island example. In Cherbourg, the German troops were isolated and demoralized, and had been the targets of previous deceptions, EW and physical attack. Again, once PSYOP was applied, a smaller force would have been able to complete the capture of the town.

As seen by both examples, PSYOP can be used to reduce the enemy's will to fight, leading to the reduction of strongpoints, with an end result being an increase in the MAGTF's operational tempo. At Faylaka Island, the objective was secured quickly,

since the Iraqis offered no resistance. This allowed the assault forces to move quickly to subsequent objectives. At Cherbourg, German resistance ceased after PSYOP took effect. This prevented the need for the further reduction of German strongpoints. The results were twofold. First, forces conducting the assault on Cherbourg could be used elsewhere. Second, repair of the port facilities could begin, allowing for additional throughput of manpower and supplies to Allied forces in France. In both examples, operational tempo was increased.

Both historical examples support the proposed doctrinal principle that PSYOP planning should be proactive, fueled by continuous intelligence and guidance from higher headquarters. In the Faylaka Island example, Iraqi troop dispositions were known, since the island had been isolated and the ATF was in the vicinity. Reports from elsewhere in the KTO informed the ATF of mass Iraqi surrenders. Finally, since the Faylaka Island example was just a small operation of a much larger campaign, the operating environment was mature. Therefore, PSYOP guidance and themes were readily available. The same holds true for the Cherbourg example. PSYOP in support of Operation Overlord was generally planned well in advance, with local modifications as required, as shown in the Second Mobile Radio Broadcast Company example. In future operations, such guidance may not be present in an unformed or developing operational environment unless a continuous intelligence process is in place. This continuous intelligence process must provide decision makers the appropriate information to ensure the MAGTF can proactively plan for the use of PSYOP. MAGTF PSYOP themes must be consistent with those of follow-on forces!

The three possible doctrinal principles for PSYOP are applicable to the most significant threat to the MAGTF ashore, that posed by the armored and artillery elements of an enemy reaction force. PSYOP, combined with the other elements of offensive IO, can target the enemy's reaction forces. One appropriate PSYOP theme could tell the reaction forces that if they respond, they will be destroyed. Other themes could be used, as required. These possible doctrinal principles are also useful for present threats across the spectrum of warfare. As seen by the two historical examples, isolated, demoralized ground combat units are particularly susceptible to PSYOP. Modified and combined with CNA, these doctrinal principles can be used against enemy IO and computer based threats.

The three doctrinal principles listed above are feasible for use by a future MAGTF if reach back is used to retrieve pertinent information. First, reach back must be used to receive PSYOP guidance from the supported JFC or CINC. This will ensure consistency of the PSYOP theme, allowing it to support the overall campaign design. Second, reach back must be used to consult experts on the themes and best methods of dissemination. These experts currently reside in the U.S. Army. This will ensure a professional, relevant product will be produced.

PSYOPs against potential enemies can be preplanned in coordination with U.S. Army assets. While deployed, reach back can be used to electronically retrieve products, which are then locally reproduced aboard ship or at the nearest land facility. The MAGTF has the delivery means to disseminate most PSYOP products.

As shown by the two historical examples, PSYOPs were used during Operation Desert Storm and Operation Overlord with effective results. A MAGTF using these

doctrinal principles will have increased combat power, greater tempo, and provide an initial PSYOP effort for follow-on forces.

Recommendations: PSYOP

Four recommendations are submitted with regard to PSYOP:

1. That the Marine Corps train MAGTF planners in PSYOP planning and execution in accordance with appendices B and E of FM 33-1 (FMFM 3-53) *Psychological Operations*. Appendix B shows how PSYOP can be used across the spectrum of conflict. Specifically, the section on “deep operations” is applicable for PSYOP against an enemy’s reaction forces. Appendix E lists the duties of the PSYOP staff officer.
2. That MAGTF intelligence sections develop procedures for and execute continuous intelligence operations while deployed. (This recommendation will be covered in greater detail later in this chapter.)
3. That the Marine Corps establish and maintain liaison and reach back capability for deployed MAGTFs with PSYOP expertise within the U.S. Army. This would include points of contact with the Army PSYOP community, and the assignment of reach back to specific MAGTF staff personnel.
4. That the MAGTF maintain the dissemination means for PSYOP products. This specifically includes loudspeakers (aerial and vehicular), radios and leaflet production/dissemination apparatus and techniques.

Conclusions: Deception

Three possible doctrinal principles are identified for the use of deception in the context of this thesis. First, to achieve deception objectives, it may be necessary to

position amphibious shipping to conduct deception operations. This may require a change in the supporting/supported relationship between the commander, amphibious task force (CATF) and the commander, landing force (CLF). The positioning of amphibious shipping to support the MAGTF's concept of operation will be required. This may include the dispersal of amphibious shipping within the ARG to a degree not currently conducted. The current command relationship establishing the CATF and CLF as coequals for planning, then the CATF assumes overall command until the CLF is established ashore will no longer be valid. Second, by using deception, MAGTF planners can plan to influence a greater number of amphibious objectives, using deception to duplicate the effects of a greater number of combat units on scene. The other units can be simulated by deception. Third, deception can spread an enemy's defensive forces laterally and in depth. The movement of amphibious forces along a coastline forces the enemy to spread his forces laterally. The increased maneuverability of the MV-22 expands the threat of amphibious landings to greater distances inland, forcing the enemy to spread his forces in depth. Additionally, the threat of airborne landings achieves even greater results. This forces greater reliance on an enemy's mobile reserve. Spreading an enemy's defense also makes them more susceptible to swarming tactics.

All three of these possible doctrinal principles are supported by both the selected historical examples. These possible doctrinal principles are applicable to the threat posed by an enemy reaction force. These possible doctrinal principles are also useful for present threats across the spectrum of warfare. Additionally, they can be used for their deterrent value to prevent crises.

As shown in the Operation Pastel historical example, by hinting at the use of several possible landings and landing sites by an amphibious force, Allied planners were able to force the Japanese to disperse their forces laterally. Although Pastel did not mature enough to use the movement of amphibious shipping to achieve deception objectives, other deception means were used, particularly radio. In the Operation Fortitude example, the positioning of seaborne and amphibious transport assets in ports were used to keep the Germans from knowing the landing areas in advance. These transport assets were spread loaded throughout the British Isles, with a heavy concentration to support Patton's phony First Army Group positioned near Pas-de-Calais. This is one example of positioning amphibious shipping to conduct deception operations; Appendix B contains several other historical examples.

Deception can be used to influence a greater number of amphibious objectives. The use of deception can duplicate the effects of a greater number of combat units on scene. In Operation Pastel, phony glider and airborne units were portrayed, and just before the Japanese surrender, planners were beginning to portray a fictional airborne corps headquarters and a division headquarters. This deception even included the production of 1,000 shoulder patches for the units (Huber 1988, 7). The proposed doctrinal principle stating that MAGTF planners can plan to influence a greater number of amphibious objectives, using deception to duplicate the effects of a greater number of combat units on scene, is also supported by the Operation Overlord Case Study. The effects of Patton's First Army Group have already been documented.

Both historical examples support the third proposed doctrinal principle for deception that deception can spread an enemy's defensive forces laterally and in depth.

As seen by Operation Pastel, the Japanese had grave concerns on the possibility of the use of airborne forces by the Allies. Allied planners played on those fears, forcing the Japanese to choose between defending at the water's edge or further inland. The Allies' use of dummy airborne insertions during the first night of the Normandy invasion, coupled with actual airborne operations, further spread the German's defensive response and increased the confusion of their leadership.

As shown by the two historical examples, deception was used in support of amphibious operations in the Pacific and European Theater of Operations during World War II. Amphibious deception can be used in numerous ways and can potentially be the element of offensive IO that can increase the combat power of a MAGTF to the greatest extent.

Recommendations: Deception

Three recommendations are submitted with regard to deception:

1. That the Marine Corps institute the procedure of using nonselected courses of action from the Marine Corps Planning Process (MCPP) for use as amphibious deception plans (Parker 1992, 101). This is an easy way to ensure the inclusion of deception in operational planning without the devotion of much additional time and resources.

According to Lieutenant General Bernard E. Trainor:

Thus, it is available for exploitation as a deception tool should the circumstances or opportunity commend it to the commander. The commander can do this by developing the rejected course of action and spuriously using it to signal intent, while he develops his preferred option under the cloak of operational secrecy. (Trainor 1986, 58)

2. That MAGTF intelligence sections develop intelligence preparation of the battlefield (IPB) procedures for identifying and exploiting the vulnerabilities to deception for

potential adversaries across the spectrum of conflict. This IPB should focus on the sensors available to the adversary. The Notional Critical Target Sets shown in table 17, Warden's Basic Five Rings Model, and more modern nodal analysis techniques serve as a starting point.

3. That the Marine Corps develop procedures to integrate deception and swarming tactics. This couples deception with physical attack/destruction and other elements of Offensive IO, which has proven so effective in the past.

Conclusions: OPSEC

One possible doctrinal principle is identified for the use of OPSEC in the context of this thesis, that is, OPSEC is critical for the success of deception. If an enemy receives several bits of information from different sources on the plans of a MAGTF, any deception is bound to fail. Conversely, the practice of good OPSEC will set the conditions for effective deception. An end result is the spreading of an enemy's defensive forces laterally and in depth.

This possible doctrinal principle is supported by the selected historical examples. As shown by the Marine Corps' Navajo Code Talker Program, secure communications and Information Assurance (IA) is required for MAGTF operations. This holds true for deception. A compromised deception operation can produce serious and possibly catastrophic consequences for the MAGTF. In Operations Olympic and Pastel, naval transmissions were to be controlled so as not to reveal that a large force was at sea before actual landings. In Operation Overlord, the Allies were successful in protecting information pertaining to when and where the landings would occur, who would conduct

the landings, and to some degree by what methods. This not only allowed for the successful Overlord landings, but the successful implementation of Fortitude as well.

It is essential that good OPSEC be practiced by the MAGTF. Good OPSEC can serve as a precaution against threats across the spectrum of warfare.

Recommendations: OPSEC

Five recommendations are submitted with regard to OPSEC:

1. That the MAGTF commander and staff ensure OPSEC planning is a continuous process (The Joint Chiefs of Staff 1997a, I-3, II-2). OPSEC planning and plan reevaluation should take place at all times when a MAGTF is preparing for deployment and while deployed. MAGTF standing operating procedures (SOPs) and TTPs should address OPSEC planning and plan reevaluation. This planning and plan reevaluation process should also be tied into the continuous intelligence operations.
2. That MAGTF training plans include an emphasis on OPSEC. This training should extend to every Sailor of the ARG.
3. That MAGTF CI personnel and intelligence sections continuously reevaluate the potential of information leaks through e-mail, the internet and cellular phones. The proliferation of such technologies is a double-edged sword!
4. That effective policies on the use of e-mail, internet and cellular phones (both government and personal) be developed, instituted and enforced within the MAGTF.
5. That the Marine Corps consider the use of a human element to augment cryptology to ensure IA on MAGTF command nets. Using electronic cryptology as a sole source of IA leaves the MAGTF vulnerable to an adversary that may compromise these assets.

Conclusions: Physical Attack or Destruction

Four possible doctrinal principles are identified for the use of physical attack or destruction in the context of this thesis. First, physical attack or destruction should be used against enemy sensors and command and control nets that initiate the mobile reserve's counterattack. Second, physical attack or destruction should be used against enemy sensors to assist with deception objectives. Third, the effects of the attacks against each target must be carefully determined and clearly understood by the attackers. This will prevent the destruction of critical infrastructure that will be needed by the MAGTF or the JTF at a later date. Additionally, the political requirement to use minimal force to reduce casualties and destruction may be in effect. In some cases, physical attack and seizure will be required instead of physical destruction. Fourth, if an enemy's defense is sufficiently spread laterally and in depth, it is susceptible to swarming tactics.

All four of these possible doctrinal principles are supported by both the selected historical examples. These possible doctrinal principles are especially applicable to the threat posed by an enemy reaction force. However, these possible doctrinal principles are also useful for present threats across the spectrum of warfare.

Operation Just Cause supports the proposed doctrinal principle stating that physical attack or destruction should be used against enemy sensors and command and control nets that initiates the mobile reserve's counterattack. Of the four categories of H-Hour targets (as classified by the author) one focused on the physical attack or destruction of targets that were the command and control of the Panamanian nation and PDF. Of the twenty-three H-Hour targets shown in table 10, ten can be classified in this category. Their physical attack or destruction paralyzed the PDF and other paramilitary

forces. This allowed for their isolation and piecemeal surrender, and prevented the use of a PDF reserve. It also prevented the organization of resistance by guerrilla warfare.

The Operation Overlord Case Study supports the second proposed doctrinal principle for physical attack or destruction stating that physical attack or destruction should be used against enemy sensors to assist with deception objectives. Physical destruction was used against the German sensors and command and control that would initiate the mobile reserve's counterattack. Physical destruction of the German's sensors allowed the successful execution of the Fortitude deception by attacking targets that were located in the Pas-de-Calais region. This prevented German sensors and commanders from gaining the true intentions of the Allies, causing the certainty that the Normandy landings were not the Allied main effort, preventing the commitment of mobile reserve forces.

Several historical examples support the third doctrinal principle stating that the effects of the attacks against each target must be carefully determined and clearly understood by the attackers. Of the four categories of H-Hour targets in Operation Just Cause, one category was Panamanian and U.S. infrastructure. These targets allowed for the unimpeded arrival of follow on forces. Of the twenty-three H-Hour targets shown in table 10, eight can be classified in this category. In most cases, the destruction of the target would have hampered the United States' ability to receive follow-on forces into Panama and to get those forces into the fight. It was imperative that all assault forces understood the necessity of not destroying these targets, that physical occupation was required. The control of many of these targets also prevented their use by the PDF to reinforce its units. In Operation Fortitude, German coastal defense radars were destroyed

in a preconceived, highly calculated pattern. Some were purposely left intact near Pas-de-Calais to ensure their use by the Germans in support of Allied EW efforts. Their destruction would have been counterproductive.

Operation Just Cause supports the proposed doctrinal principle that if an enemy's defense is sufficiently spread laterally and in depth, it is susceptible to swarming tactics. In Panama, a series of near simultaneous attacks at H-Hour against an enemy's command and control, troop concentrations, and reinforcement capability was very effective. In this instance, several of the categories of Warden's Five Rings Model (figure 3) were attacked at once. The results are common knowledge.

As shown by historical examples, the use of physical attack or destruction against an enemy's command and control, troop concentrations, and reinforcement capability in conjunction with other elements of offensive IO increases the combat power of the attacking force.

Recommendations: Physical Attack or Destruction

Four recommendations are submitted with regard to physical attack or destruction:

1. That Marine Corps doctrinal terminology change from Physical Destruction to Physical Attack or Destruction. This more accurately reflects the range of combat actions that can be taken against an enemy target. Often, enemy assets targeted for physical attack in support of IO objectives will be seized or secured instead of destroyed because of their future value.
2. That Colonel John A. Warden's Five Rings Model and more modern nodal analysis techniques are further studied as ways to better target an enemy's mobile reserve force and determine other amphibious objectives.

3. That MAGTF intelligence sections develop procedures for identifying the location of an enemy's mobile reserve force and its command and control vulnerabilities that can be exploited. Again, the Notional Critical Target Sets shown in table 17, Warden's Basic Five Rings Model, and more modern nodal analysis serve as starting points.
4. Again, that the Marine Corps develop procedures to integrate deception and swarming tactics.

Conclusions: EW

No possible doctrinal principles are identified for the use of EW in the context of this thesis. EW can be used to support and compliment the other elements of offensive IO against enemy sensors and command and control nets that initiates the mobile reserve's counterattack and against critical infrastructure that will be used by the mobile reserve for counterattack routes. Additionally, EW can be used to support swarming tactics.

Recommendations: EW

One recommendation is submitted with regard to EW:

1. That the Marine Corps develop procedures to ensure the integration of EW in support of swarming tactics.

Conclusions: CNA Liaison

No potential doctrinal principles are identified for the use of CNA Liaison in the context of this thesis. However, as with EW, CNA can be used to support and compliment the other elements of offensive IO as shown above. Additionally, along with EW, CNA can be used to support swarming tactics. As shown by the historical example,

and the use of CNA against certain enemy's targets in conjunction with other elements of offensive IO increases the combat power of a MAGTF.

Recommendations: CNA Liaison

Four recommendations are submitted with regard to CNA Liaison:

1. That the Marine Corps train MAGTF planners in CNA Liaison. The MAGTF must have the resident planning knowledge to integrate the combat multiplier of CNA into traditional amphibious and expeditionary operations.
2. That the Marine Corps establish and maintain liaison and reach back capability for deployed MAGTFs with JTF CNA or other commands and agencies charged with CNA responsibilities.
3. That the Marine Corps develop procedures to integrate CNA in support of swarming tactics.
4. As stated in chapter two, this thesis recommends that the Marine Corps doctrinal element of offensive IO, Computer Network Attack, be modified to Computer Network Attack Liaison.

Conclusions: Support to SIO

No potential doctrinal principles are identified for support to SIO in the context of this thesis. However, because of their forward-deployed nature and inherent flexibility, MAGTFs must be able to support such SIOs in the future.

Recommendations: Support to SIO

Three recommendations are submitted with regard to Support to SIO:

1. As stated in chapter two, this thesis recommends that Support to SIO be added to the elements of offensive IO for the Marine Corps. Because of their forward-deployed nature and inherent flexibility, MAGTFs must be able to support such SIOs in the future. The use of MAGTF aviation, EW, and other assets may be used to take advantage of any fleeting opportunities created by the United States' control of information.
2. It is possible for tactically oriented SIOs to be mounted against the leadership of an adversary's military, and specifically the leadership of an enemy's coastal defenses and/or mobile reserves in the future. The Marine Corps should consider developing procedures for such operations to take advantage of emerging technologies.
3. Because of their forward-deployed nature, MAGTFs may support SIOs in the realm of diplomatic deception in the future. The use of the MAGTF's command element, as well as its mobile training team (MTT) capability and ability to conduct training exercises with the militaries of other nations, allows for the forum of supporting diplomatic deception. Again, the Marine Corps should consider developing procedures for such operations, to include reach back procedures for the diplomatic deception theme, much like the PSYOP theme in an unformed or developing operational environment.

Additional Conclusions and Recommendations

In addition to the conclusions and recommendations listed above for each element of offensive IO, one proposed doctrinal principle requires expansion, and one recommendation for MAGTF intelligence procedures is offered.

First, a proposed doctrinal principle covered under PSYOP is that MAGTF intelligence sections emphasize continuous intelligence operations while deployed.

Although included in PSYOP, this principle is overarching and applies to each element of offensive IO. Continuous intelligence has become a reality and requirement in the Information Age. Joint Publication 3-02, *Joint Doctrine for Amphibious Operations*, states:

Successful accomplishment of the ATF [amphibious task force] mission is dependent on timely and accurate intelligence. Intelligence planners must direct the intelligence collection effort toward the preparation of an estimate of the situation that supports decisionmaking regarding what will be done as well as when, where, how, and why. The collection effort is continuous throughout the amphibious operation and involves collection agencies from the national level down to the individual service member. (The Joint Chiefs of Staff 1992, IV-1)

Joint Publication 3-02 further states: "CATF, working closely with CLF, coordinates the collection process to ensure integration of effort, expeditious collection, rapid processing, and prompt dissemination of intelligence" (The Joint Chiefs of Staff 1992, IV-1).

FM 34-1, *Intelligence and Electronic Warfare Operations*, states that the Intelligence Battlefield Operating System (BOS) is always engaged.

The Intelligence BOS is always engaged. Through continuous peacetime intelligence operations, commanders ensure collection, processing, analysis, and dissemination infrastructure is in place and prepared to provide intelligence support throughout the range of military operations. Early intelligence preparation is critical to the commander's decision making and planning process for force projection operations. The commander and G-2 (S-2) must assess each contingency to determine intelligence requirements and develop a plan for filling

intelligence voids. The primary feature is tempered, however, by the imperative to prioritize efforts and prepare thoroughly for top priority contingency areas. (Headquarters, Department of the Army 1994 1-11 and 1-12)

Since the MAGTF may frequently respond to an unformed or developing operational environment, the above quote from FM 34-1 is quite applicable.

In his essay, "The Revolution in Military Affairs: The Information Dimension," Michael L. Brown reflects this continuous need of intelligence in a figure he entitles Time and Command, shown in table 16.

Table 16.

Time and Command.

	Revolution	Civil War	WW II	Gulf War	Tomorrow
<i>Orientation</i>	Telescope	Telegraph	Radio/wire	Near real-time	Real-time
<i>Observation</i>	Weeks	Days	Hours	Minutes	Continuous
<i>Decision</i>	Months	Weeks	Days	Hours	Immediate
<i>Action</i>	Season	A month	A week	A day	Hour or less

Source: Brown, Michael L. 1996. "The Revolution in Military Affairs: The Information Dimension." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press, 34.

The MAGTF intelligence sections of the future must emphasize continuous intelligence operations while deployed. These intelligence operations must include likely adversaries within the range of the MAGTF, while ranging the entire spectrum of conflict. Future MAGTF operations will occur so rapidly that intelligence sections cannot start their intelligence studies of the newly arisen adversary from scratch. The challenge for MAGTF intelligence personnel includes information management,

prioritization, dissemination, and the limits of intelligence personnel in the MAGTF troop list. Innovation and organization will be required to produce intelligence sections capable of continuous intelligence operations.

In his essay “Strategic Information Warfare and Comprehensive Situational Awareness,” Daniel T. Kuehl offers some notional critical target sets. Shown in table 17, these notional target sets provide a good starting point for MAGTF intelligence personnel in developing IPB procedures for identifying and exploiting the vulnerabilities to offensive IO for potential adversaries across the spectrum of conflict.

Comparison of Proposed Doctrinal Principles to Existing Doctrine

All proposed doctrinal principles are informally compared to existing joint doctrine to ensure there is little, if any, duplication. Additionally, they are compared to the principles of OMFTS to ensure doctrinal consistency. Criteria used to determine the most necessary and useful elements are the principles of OMFTS, which were shown in table 2 of this thesis.

In comparing the three possible PSYOP doctrinal principles to the principles of OMFTS, each focuses on an operational objective, assists in the generation of overwhelming combat power, pits strength against weakness, emphasizes intelligence, deceptions, and flexibility, and integrates joint assets. Additionally, these three possible doctrinal principles are consistent with, and compliment, the principles of joint PSYOP as listed below:

1. The PSYOP mission must be clearly defined in terms that correspond to the supported commander’s vision of how the campaign or operation will proceed.

Table 17.

Notional Critical Target Sets.

<p><u>Political</u></p> <ul style="list-style-type: none">• National governmental apparatus and centers<ul style="list-style-type: none">▣ Headquarters, administrative offices, and ministries▣ Supporting command, control, communications (C3) nodes (hard or soft)▣ Command posts (mobile/fixed; air/land/at sea)• Internal state police and control forces<ul style="list-style-type: none">▣ Headquarters, intelligence technical collection systems▣ Supporting databases• Propaganda systems: domestic and international<ul style="list-style-type: none">▣ Public affairs, public diplomacy, and PSYOP organizations and production facilities▣ Cultural centers/networks▣ Links into area/international telecommunications nets <p><u>Infrastructure</u></p> <ul style="list-style-type: none">• Information infrastructure<ul style="list-style-type: none">▣ Public and secure telecommunications switches▣ Radio relay facilities and telephone exchanges▣ Fiber optic networks, nodes, and repeater stations▣ Microwave transmission networks and nodes▣ Computer and data processing centers▣ National command, control, communications, intelligence (C3I) centers and satellite communications (SATCOM) links• Energy and power sources<ul style="list-style-type: none">▣ Production centers, transformer stations, distribution and control centers▣ Pumping stations and backup systems• Transportation<ul style="list-style-type: none">▣ Ground traffic control at chokepoints▣ Air traffic control centers▣ Supporting computer and electronic systems• Financial centers and networks<ul style="list-style-type: none">▣ Banks and trading centers and institutions▣ Currency controls and depositories and supporting databases• Population stability<ul style="list-style-type: none">▣ Food and water distribution systems and control points <p><u>Military Forces</u></p> <ul style="list-style-type: none">• Strategic national defenses<ul style="list-style-type: none">▣ Warning systems sensors▣ Defense command and control centers▣ SATCOM links to space-based systems▣ Deployed forces• Strategic offensive force projection systems<ul style="list-style-type: none">▣ Conventional delivery systems▣ Unconventional weapons systems▣ Control centers, command posts, research and development centers
--

Source: Kuehl, Daniel L. 1996. "Strategic Information Warfare and Comprehensive Situational Awareness." In *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press, 192.

2. PSYOP themes, activities, and symbols should be based on a thorough analysis of targets, including friendly and adversary PSYOP capabilities, strengths, and weaknesses.
3. All military actions should be thoroughly evaluated for their psychological implications and, where necessary, supported by deliberate PSYOP actions to offset potentially negative effects or to reinforce positive effects.
4. The medium or media selected for transmission should be reliable and readily accessible by target audiences.
5. Rapid exploitation of PSYOP themes is often critical. Planning, pretesting, and approval procedures should be developed to exploit fleeting opportunities.
6. Where possible, the results of PSYOP should be continually evaluated for relevance to the mission and to national and military goals. As with initial planning actions, decisions to terminate or revise PSYOP programs must be linked to careful analysis of all-source intelligence (The Joint Chiefs of Staff 1996b, I-2, I-3).

In comparing the three possible deception doctrinal principles to the principles of OMFTS, each focuses on an operational objective, potentially generates overwhelming combat power, pits strength against weakness, emphasizes intelligence, deceptions, and flexibility; integrates all organic, joint, and combined operations, and potentially the most critical, these three possible doctrinal principles use the sea (and air) as maneuver space. Additionally, these three possible doctrinal principles are consistent with, and compliment, the joint principles of deception as listed below:

1. **Focus.** The deception must target the adversary decision maker capable of taking the desired action(s). The adversary's intelligence system is normally not the target. It is only the primary conduit used by deceivers to get selected information to the decision maker.
2. **Objective.** The objective of the deception must be to cause an adversary to take (or not to take) specific actions, not just to believe certain things.
3. **Centralized Control.** A deception operation must be directed and controlled by a single element. This approach is required in order to avoid confusion and to ensure that the various elements involved in the deception are portraying the same story and are not in conflict with other operational objectives.
4. **Security.** Knowledge of a force's intent to deceive and the execution of that intent must be denied to adversaries. Successful deception operations require strict security.
5. **Timeliness.** A deception operation requires careful timing. Sufficient time must be provided for its portrayal; for the adversary's intelligence system to collect, analyze, and report; for the adversary decision maker to react; and for the friendly intelligence system to detect the action resulting from the adversary decision maker's decision.
6. **Integration.** Each deception must be fully integrated with the basic operation that it is supporting. The development of the deception concept must occur as part of the development of the commander's concept of operations. Deception planning should occur simultaneously with operation planning (The Joint Chiefs of Staff 1996b I-3).

In comparing the possible OPSEC doctrinal principle to the principles of OMFTS, it focuses on an operational objective and emphasizes intelligence, deceptions, and flexibility.

In comparing the six possible physical attack doctrinal principles to the principles of OMFTS, each focuses on an operational objective, attempts to generate overwhelming combat power, pits strength against weakness, emphasizes intelligence, and integrates organic, joint and combined operations.

Answers to the Primary and Secondary Research Questions

This thesis answered the primary research question: What are the doctrinal principles that will enable the MAGTF to conduct offensive information operations in a littoral region with an unformed or developing, operational environment? These proposed doctrinal principles were identified in chapter five and are summarized in table 18.

Several subordinate questions were answered in this thesis. First, the elements of IO in accordance with the current Marine Corps Concept Paper on Information Operations were identified in chapter two of this thesis. Existing and emerging threats to the MAGTF's ability to conduct offensive operations in the future were identified in chapter three. The most significant threat to the MAGTF ashore will be posed by the armored and artillery elements of an enemy reaction force. Based on historical examples, the question to determine if the proposed doctrinal principles of IO add to the combat power of the MAGTF was answered in chapters four and five. The identification of the most necessary and useful elements of offensive IO for a MAGTF occurred in chapter five. The elements of offensive IO that can be used most often, with the most flexibility and imagination are deception and OPSEC.

Table 18.

Proposed Doctrinal Principles in the Employment of Offensive IO by the MAGTF.

1. PSYOP should be considered in all potential operations, it is a proven combat multiplier.
2. PSYOP can be used to reduce the enemy's will to fight. It can reduce strongpoints and increase a MAGTF's operational tempo.
3. PSYOP themes must be consistent with future JTF commanders and the CINC's desires.
4. To achieve deception objectives, it may be necessary to position amphibious shipping to conduct deception operations. This may require a change in the supporting/supported relationship between the CATF and the CLF.
5. By using deception, MAGTF planners can plan for the use of one-third to double the combat units on scene.
6. Deception can spread an enemy's defensive forces laterally and in depth.
7. OPSEC is critical for the success of deception.
8. Physical attack or destruction should be used against enemy sensors and command and control nets that initiates the mobile reserve's counterattack.
9. Physical attack or destruction should be used against critical infrastructure that will be used by the mobile reserve for counterattack routes.
10. Physical attack or destruction should be used against enemy sensors to assist with deception objectives.
11. When planning physical attack or destruction missions, the effects of the attacks against each target must be carefully determined and clearly understood by the attackers. This will prevent the destruction of critical infrastructure that will be needed by the MAGTF or the JTF at a later date.
12. If an enemy's defense is sufficiently spread laterally and in depth, it is susceptible to swarming tactics.
13. That MAGTF intelligence sections emphasize continuous intelligence operations while deployed.

Significance of Thesis

This thesis is significant in that it proposes new doctrinal principles in the employment of offensive IO. Such employment is enables the increase of the deterrence capability, flexibility, and overall combat power of the MAGTF. These proposed principles are more specific than current joint doctrine and are based on successful historical examples.

Relationship to Previous Studies

There is no evidence to suggest that a similar type of study has been conducted on the elements of offensive IO in relation to the MAGTF. This thesis is an attempt to provide a link between the concept paper *A Concept for Information Operations*, which supports Operational Maneuver From the Sea, and the TTPs required by the MAGTF to take advantage of the potential combat power that offensive IO provides.

Suggestions for Further Study

The focus of the thesis was on the identification of proposed doctrinal principles for the elements of offensive IO. The information drawn from the analysis of the elements of offensive IO leads me to believe that the same type of study should be conducted for the elements of defensive IO, since the two sets of elements of IO are interrelated. A study that ensures integration of the two sets of elements of IO should follow that effort. Additionally, proposed TTPs for both the offensive and defensive elements of IO should be developed for the MAGTF. Appendix B of this thesis provides other relevant historical examples for studying the elements of offensive IO and their potential uses by the MAGTF. These examples can also be of use for studying the defensive elements of IO and developing TTPs. Finally, the threat analyzed in this thesis remained largely at the conventional, medium intensity level of the spectrum of conflict. Further research should be conducted in for proposed doctrinal principles and TTPs for threats that include terrorists and other nonstate actors, as well as MOOTW scenarios.

Thesis Summary

The ability for MAGTFs to effectively conduct offensive IO in the future is critical. Offensive IO will be a force multiplier for deployed forces, which by mobility

requirements and resource shortages, are austere and lean by nature. Additionally, offensive IO may prove to be very effective against the myriad of existing and emergent threats, with their increased lethality and reliance on asymmetrical warfare. The Marine Corps must prepare offensive IO doctrine to assist MAGTF personnel in the conduct of offensive IO.

This thesis proposes doctrinal principles of the employment of offensive IO that are more specific than current joint doctrine and are based on successful historical examples. These proposed doctrinal principles are specific to a littoral region with an unformed or developing operational environment, a operational environment that is most often the operating area for a forward deployed MAGTF. These proposed doctrinal principles support OMFTS and provide a link between the Marine Corps Concept Paper on Information Operations and actual operating procedures.

APPENDIX A

DEFINITIONS

- Asymmetrical Threat.** The potential of attack from unconventional, unexpected, innovative or disproportional means (Preliminary Coordinating Draft, Joint Publication 1-02, 19 February 1999).
- Asymmetry.** Unconventional, unexpected, innovative or disproportional means used to gain advantage over an adversary (Preliminary Coordinating Draft, Joint Publication 1-02, 19 February 1999). Violence with a paramilitary goal (MCIA *Midrange Threat Estimate 1997-2007*).
- Deception Operations.** A military operation conducted to mislead the enemy (FM 101-5-1/MCRP 5-2A).
- Defensive Information Operations.** The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems. This includes information assurance, operational security (OPSEC), physical security, counterdeception, counterpropaganda, counterintelligence, electronic warfare (EW), and special information operations (SIO) (Joint Publication 3-13).
- Developing Operational Environment.** An operational environment in which the Joint, multinational, and interagency linkages, the circumstances of the operational environment, are being developed (FM 100-7).
- Doctrinal Principle.** "Doctrine" is the fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application (Joint Publication 1-02). "Principle" is defined as a "general or fundamental law" (Webster's Dictionary).
- Information Assurance (IA).** "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (Joint Publication 3-13).
- Littoral Environment.** The area where land and sea meet. This is where seaborne trade originates and terminates. The littorals include straits, most of the world's population centers, and the areas of future maximum growth (MCDP 3).

Marine Air-Ground Task Force (MAGTF). A task organization of Marine forces (division, aircraft wing, and service support groups) under a single command and structured to accomplish a specific mission. The MAGTF components will normally include command, aviation combat, ground combat, and combat service support elements (including Navy Support Elements) (FM 100-5-1/MCRP 5-2A).

Marine Expeditionary Brigade (MEB). A task organization that is normally built around a regimental landing team, a provisional Marine aircraft group, and a logistics support group. This brigade-sized unit can be designated as the lead echelon of the MEF, or it can operate independently in contingencies of a lesser scale.

Marine Expeditionary Force (MEF). The Marine Expeditionary Force, the largest of the Marine Air-Ground Task Forces, is normally built around a division/wing team, but can include several divisions and aircraft wings, together with an appropriate combat service support organization. (FM 100-5-1/MCRP 5-2A)

Marine Expeditionary Unit (MEU). A task organization that is normally built around a battalion landing team, reinforced helicopter squadron, and logistics support unit. It fulfills routine afloat forward deployment requirements, provides an immediate reaction capability for crisis situations, and is capable of relatively limited combat operations (FM 100-5-1/MCRP 5-2A).

Marine Expeditionary Unit (Special Operations Capable) [MEU (SOC)]. A forward-deployed, embarked unit with enhanced capability to conduct special operations. It is oriented toward amphibious raids, at night, under limited visibility, while employing emission control procedures. The MEU (SOC) is not a Secretary of Defense-designated special operations force but, when directed by the National Command Authorities and/or the theater commander, may conduct hostage recovery or other special operations under in extremis circumstances when designated special operations forces are not available (Joint Publication 1-02).

Operational Environment. A composite of the conditions, circumstances, and influences that affect the employment of military forces and bear on the decisions of the unit commander (Joint Publication 1-02).

Operational Maneuver from the Sea (OMFTS). An approach to expeditionary, littoral, and amphibious warfare. It is the maneuver of naval forces at the operational level, a bold bid for victory that aims at exploiting a significant enemy weakness in order to deal a decisive blow (OMFTS Concept Paper).

Reach Back. The use of organic and external staffs and subject matter experts which are out of the immediate operating area or even theater of war. Use of reach back personnel reduces in-theater security requirements and reduces the command

elements footprint (both ashore and at sea). It also provides a broader, diverse experience base (MCWP 0-1 Final Draft of 25 June 1999).

Special Purpose MAGTF (SPMAGTF). A non-standing MAGTF temporarily formed to conduct a specific mission. It is normally formed when a standing MAGTF is either inappropriate or unavailable (MCRP 5-12D).

Theater of Operations. A subarea within a theater of war defined by the geographic combatant commander required to conduct or support specific combat operations. Different theaters of operations within the same theater of war will normally be geographically separate and focused on different enemy forces. Theaters of operations are usually of significant size, allowing for operations over extended periods of time (Joint Publication 1-02).

Unformed Operational Environment. An operational environment in which the Joint, multinational, and interagency linkages, the circumstances of the operational environment, are not formed. An unformed operational environment is considered "worst case" (FM 100-7).

APPENDIX B

ADDITIONAL HISTORICAL EXAMPLES

Other relevant historical examples in studying the elements of offensive Information Operations and their potential uses by the MAGTF are shown in tables 19 through 24.

Table 19.

Additional Historical Examples, PSYOP.

Example	Reference(s)
Belated use of PSYOP in Grenada, Operation Urgent Fury	(1) Cole, Robert H. <i>Operation Urgent Fury, The Planning and Execution of Joint Operations in Grenada, 12 October – 2 November 1983</i> . Washington DC: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff, 1997, 16, 50-51, 67. (2) U.S. Army Special Operations Command, Directorate of History and Museums. <i>A History of U.S. Army Combat Psychological Operations</i> , 364-369.
Use of PSYOP in Haiti, U.S. Army, Operation Uphold Democracy	(1) Brown, Stephen D. "PSYOP in Operation Uphold Democracy." <i>Military Review</i> , September-October 1996, 57-73. (2) Kretchik, Walter E., Baumann, Robert F., Fishel, John T. <i>Invasion, Intervention, "Intervention": A Concise History of the U.S. Army in Operation Uphold Democracy</i> . Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 1998, 125-130.
Use of PSYOP in Bosnia, U.S. Army	Siegel, Pascale Combelles. <i>Target Bosnia: Integrating Information Activities in Peace Operations. NATO-Led Operations in Bosnia-Herzegovina, December 1995-1997</i> . Washington DC: DoD Command and Control Research Program, Institute for National Strategic Studies, 1998, 67-106.

Table 20.

Additional Historical Examples, Deception.

Example	Reference(s)
Deception operations in the Battle of El Alamein; British Army, World War Two (good TTPs)	(1) Cruickshank, Charles. <i>Deception in World War II</i> . Oxford: Oxford University Press, 1979, 19-33. (2) Majdalany, Fred. <i>The Battle of El Alamein</i> . Philadelphia: J.B. Lippencott Co., 1965, 75, 77, 119-120, 123-124. (3) Phillips, C.E. Lucas. <i>Alamein</i> . Boston: Little, Brown and Co., 1962, 132-134.
Amphibious feint against Hansa Bay, with actual landings at Hollandia (Operation Reckless); U.S. Army, World War Two	Drea, Edward J. "Audacious But Hardly Reckless." <i>Army</i> . April 1994, 50-55.
Choiseul diversion to conceal assault on Bougainville, U.S. Marine Corps, World War Two	Trainor, Bernard E. (LtGen, USMC), "Deception." <i>Marine Corps Gazette</i> , Quantico, VA: Marine Corps Association, October 1986, 57-61.
Amphibious feint against Tanapag Harbor of Saipan, with actual landings further south.	Hoffman, Carl W. <i>Saipan: The Beginning of the End</i> . Washington DC: Historical Division, U.S. Marine Corps, 1950, 45-53.
Amphibious feint to the southern beaches of Tinian, with actual landings on the northwestern beaches; U.S. Marine Corps, World War Two	Isley, Jeter A. and Crowl, Philip A. <i>The U.S. Marines and Amphibious War: Its Theory, and Its Practice in the Pacific</i> . Princeton, New Jersey: Princeton University Press, 1951, 351-359.
Operation Bluebird, deception operation to convince the Japanese that Formosa and South China would be invaded after Iwo Jima instead of Okinawa, U.S. Forces, World War Two	Parker, Robert R. Jr. (Major, USMC), "Deception: The Missing Tool." <i>Marine Corps Gazette</i> , Quantico, VA: Marine Corps Association, May 1992, 97-101.
Amphibious feint to the southeastern beaches of Okinawa, with actual landings on the western beaches, U.S. Marine Corps, World War Two	Appleman, Roy E. et al. <i>Okinawa: The Last Battle</i> . Washington DC: Historical Division, Department of the Army, 1948, 28, 33, 74, Map No. 6.
Use of 4th and 5th MEBs off the coast of Kuwait to convince the Iraqis of a pending amphibious assault, CINCENT, Persian Gulf War	Parker, Robert R. Jr. (Major, USMC). "Deception: The Missing Tool." <i>Marine Corps Gazette</i> , Quantico, VA: Marine Corps Association, May 1992, 97-101.
Choiseul diversion to conceal assault on Bougainville, U.S. Marine Corps, World War Two	Trainor, Bernard E. (LtGen, USMC), "Deception." <i>Marine Corps Gazette</i> , Quantico, VA: Marine Corps Association, October 1986, 57-61.

Table 21.

Additional Historical Examples, OPSEC.

Example	Reference(s)
Operation Compass, surprise offensive into Libya, British Army, North Africa campaign, World War Two	Savoie, Thomas A. "Deception at the Operational Level of War." <i>Army</i> . April 1987, 30-40.
Japanese OPSEC surrounding the development of a shallow water torpedo for the attack on the U.S. Pacific Fleet in Pearl Harbor	(1) Slackman, Michael. <i>Target: Pearl Harbor</i> . Honolulu: University of Hawaii Press, 1990, 15, 22. (2) Richardson, James O. <i>On the Treadmill to Pearl Harbor. The Memoirs of Admiral James O. Richardson, USN (Retired)</i> , as told to Vice Admiral George C. Dye, USN (Retired). Washington, DC: Naval History Division, Department of the Navy, 1973, 362-363.

Table 22.

Additional Historical Examples, EW.

Example	Reference(s)
Wild Weasel Program in Vietnam against North Vietnamese surface-to-air missiles	(1) <i>Wild Weasel I: Response to a Challenge</i> . USAF Southeast Asia Monograph Series, Maxwell Air Force Base, Alabama, Air War College, 1977. (2) Hewitt, William A. <i>Planting the Seeds of SEAD, The Wild Weasel Program in Vietnam</i> . School of Advanced Airpower Studies Thesis. Maxwell Air Force Base, Alabama, Air University Press, June 1993.
Ruse where F-4s Phantoms portrayed slower attack aircraft to induce MiGs to engage in air-to-air combat	Rendall, Ivan. <i>Rolling Thunder. Jet Combat from World War II to the Gulf War</i> . New York: The Free Press, 1997, 135-137.

Table 23.

Additional Historical Examples, CNA.

Example	Reference(s)
Cyberwar	<p>(1) Arquilla, John and Ronfeldt, David, <i>In Athena's Camp, Preparing for Conflict in the Information Age</i>. Santa Monica, CA: National Defense Research Institute, Rand Corporation, 1997.</p> <p>(2) Campen, Alan D., et al. <i>Cyberwar: Security, Strategy, and Conflict in the Information Age</i>. Fairfax, VA: Armed Forces Communications and Electronics Association (AFCEA) International Press, 1996.</p>
Use of internet by Zapatista guerillas, Mexico, 1990s	<p>Ronfeldt, David and Martinez, Armando. "A Comment on the Zapatista 'NetWar'." <i>In Athena's Camp, Preparing for Conflict in the Information Age</i>, edited by Arquilla, John and Ronfeldt, David. Santa Monica, CA: National Defense Research Institute, Rand Corporation, 1997.</p>

Table 24.

Additional Historical Examples, SIOs.

Example	Reference(s)
<p>“Operation Mincemeat,” “The Man Who Never Was.” (ruse used by British to convince Axis that the Allies were to invade somewhere else other than Sicily, World War Two)</p>	<p>(1) Haswell, Jock. <i>D-Day: Intelligence and Deception</i>. New York: New York Times Book Inc., 1979, 35. (2) Cruickshank, Charles. <i>Deception in World War II</i>. Oxford: Oxford University Press, 1979, 52-53.</p>
<p>Ferret Force in Malaysia (special operations unit targeting insurgent leadership)</p>	<p>Cable, Larry E. <i>Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War</i>. New York: New York University Press, 1986, 77.</p>
<p>Quang Ngai Special Platoons in Vietnam (special operations unit targeting insurgent leadership)</p>	<p>Cable, Larry E. <i>Conflict of Myths: The Development of American Counterinsurgency Doctrine and the Vietnam War</i>. New York: New York University Press, 1986, 261.</p>
<p>U.S. SOF targeting General Mohammed Aidid, Somalia, 1993</p>	<p>(1) DeLong, Kate and Tuckey, Steven. <i>Mogadishu! Heroism and Tragedy</i>. Westport, CT: Prager, 1994, xviii, 7-8. (2) Knigge, Timothy M. (MAJ, USA) <i>Operation Casablanca, Nine Hours of Hell! The Story of American Combat in Somalia</i>. Chapel Hill, NC: Professional Press, 1995, 5.</p>

REFERENCE LIST

- Addington, Larry H. 1994. *The Patterns of War Since the Eighteenth Century, Second Edition*. Bloomington, IN: Indiana University Press.
- Adolph, Robert B. Jr., Major, USA. 1992. PSYOP: Gulf War Force Multiplier. *Army*, December 1992.
- Agawa, Hiroyuki. 1979. *The Reluctant Admiral. Yamamoto and the Imperial Navy*. Tokyo: Kodansha International.
- Allen, Thomas B., and Norman Polmar. 1995. *Code-Name Downfall. The Secret Plan to Invade Japan – and Why Truman Dropped the Bomb*. New York: Simon & Schuster.
- Arquilla, John, and David Ronfeldt. 1997. *In Athena's Camp, Preparing for Conflict in the Information Age*. Santa Monica, CA: National Defense Research Institute, Rand Corporation.
- Associated Press Newswire. 1999. Military chief says US made computer attacks on Yugoslavia. 8 October, 1.
- Bixler, Margaret T. *Wings of Freedom, The Story of the Navajo Code Talkers of World War II*. Darien, CT: Two Bytes Publishing Company, 1992.
- Bradley, Omar N. General, USA. 1951. *A Soldier's Story*. New York: Henry Holt & Company.
- Breuer, William B. 1993. *Hoodwinking Hitler: The Normandy Deception*. Westport, CT: Praeger.
- Brown, Anthony C. 1965. *Bodyguard of Lies*. New York: Harper & Row.
- Brown, Michael L. 1996. The Revolution in Military Affairs: The Information Dimension. In *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press.
- Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden, ed. *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press, 1996.
- Casey, William. *The Secret War Against Hitler*. Washington, DC: Regnery Gateway, 1988.

- Cole, Robert H. 1995. *Operation Just Cause, The Planning and Execution of Joint Operations in Panama, February 1988--January 1990*. Washington DC: Joint History Office, Office of the Chairman of the Joint Chiefs of Staff.
- Cruickshank, Charles. *Deception in World War II*. Oxford: Oxford University Press, 1979.
- Davis, Burke. 1969. *Get Yamamoto*. New York: Random House.
- Department of Army, Office of Public Affairs. 1989. *Soldiers in Panama: Stories of Operation Just Cause*. Washington, DC: Department of Army.
- Department of Defense. 1992. *Final Report to Congress: Conduct of the Persian Gulf War*. Washington, DC: U.S. Government Printing Office, April 1992.
- Donnelly, Thomas, Margaret Roth, and Caleb Baker. *Operation Just Cause: The Storming of Panama*. New York: Lexington Books, 1991.
- Flanagan, Edward M. Jr. LtGen, USA. 1993. *Battle for Panama, Inside Operation Just Cause*. McLean, VA: Brassey's.
- Fox, David J. 1969. *The Research Process in Education*. New York: Holt, Rinehart and Winston, Inc.
- Glines, Carroll V. 1990. *Attack on Yamamoto*. New York: Orion Books.
- Goldstein, Frank L. Colonel, USAF. 1996. The Libyan Raid as a Psychological Operation. In *Psychological Operations, Principles and Case Studies*. Maxwell Air Force Base, Alabama: Air University Press.
- Hammond, William M. *Normandy: The U.S. Army Campaigns of World War II*. U.S. Army Center of Military History, Center of Military History Publication 72-18.
- Haswell, Jock. 1979. *D-Day: Intelligence and Deception*. New York: Times Books.
- Headquarters, Department of the Army. Field Manual 33-1 (Fleet Marine Force Manual 3-53), *Psychological Operations*. Washington, DC: U.S. Government Printing Office, 18 February 1993.
- _____. Field Manual 34-1, *Intelligence and Electronic Warfare Operations*. Washington, DC: U.S. Government Printing Office, 27 September 1994.
- _____. Field Manual 100-6, *Information Operations*. Washington, DC: U.S. Government Printing Office, August 1996.

_____. Field Manual 100-7, *Decisive Force: The Army in Theater Operations*. Washington, DC: U.S. Government Printing Office, May 1995.

_____. Field Manual 101-5-1 (Marine Corps Reference Publication 5-2A). *Operational Terms and Graphics*. Washington, DC: U.S. Government Printing Office, 30 September 1997.

Headquarters, United States Marine Corps. *Operational Maneuver from the Sea, A Concept for the Projection of Naval Power Ashore*. Washington, DC: United States Marine Corps, June 1996.

_____. Marine Corps Doctrinal Publication 1, *Warfighting*. Washington, DC: United States Marine Corps, 20 June 1997.

_____. Marine Corps Doctrinal Publication 3, *Expeditionary Operations*. Washington, DC: United States Marine Corps, 16 April 1998.

_____. Marine Corps Reference Publication 5-12D, *Organization of Marine Corps Forces*. Washington, DC: United States Marine Corps, 13 October 1998.

_____. Marine Corps Order (MCO) 3430.8, Policy for Information Operations. Washington, DC: United States Marine Corps, 19 May 1997.

_____. *Navajo Code Talkers Page*. Headquarters Marine Corps, History and Museums Division, Reference Section, March 1998, <http://www.usmc.mil/historical.nsf/Nav5>.

Headquarters, VII Corps. *Plan of Operations VII Corps: Neptune*. U.S. Army, VII Corps, APO 307: 27 March 1944.

_____. *History of the VII Corps for the Period of 6-30 June 1944, Incl (Report after action against the enemy)*. U.S. Army, VII Corps, APO 307: 23 July 1944.

_____. *Amendment Number 1 to G-2 Report Number 4*. U.S. Army, VII Corps, vicinity Audonville, La Hubert: 9 June 1944.

Headquarters, XVIII Airborne Corps. *870-5a Organizational History Files. XVIII Airborne Corps. 1989-90. Operation JUST CAUSE. Corps Historian's Notes. Notebook #1*, U.S. Army, XVIII Airborne Corps, Fort Bragg, NC, 1990.

Hillway, Tyrus. 1964. *Introduction to Research*, 2d ed. Boston: Houghton Mifflin Company.

- Hoyt, Edwin P. 1990. *Yamamoto. The Man Who Planned Pearl Harbor*. New York: McGraw-Hill.
- Huber, Thomas M. Dr. 1988. *Pastel: Deception in the Invasion of Japan*. Fort Leavenworth, KS: Combat Studies Institute, U.S. Army Command and General Staff College, December 1988.
- Hundley, Richard O. and Robert H. Anderson. 1997. Emerging Challenge: Security and Safety in Cyberspace. In *In Athena's Camp, Preparing for Conflict in the Information Age*. Santa Monica, CA: National Defense Research Institute, Rand Corporation.
- Institute for National Strategic Studies. 1999. *Strategic Assessment 1999: Priorities for a Turbulent World*. Washington, DC: National Defense University.
- The Joint Chiefs of Staff. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*. Washington, DC: The Joint Staff, 23 March 1994, as amended through 9 April 1997.
- _____. Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms (Preliminary Coordinating Draft)*. Washington, DC: The Joint Staff, 19 February 1999.
- _____. Joint Publication 3-02, *Joint Doctrine for Amphibious Operations*. Washington, DC: The Joint Staff, 8 October 1992.
- _____. Joint Publication 3-13, *Joint Doctrine for Information Operations*. Washington, DC: The Joint Staff, 9 October 1998.
- _____. Joint Publication 3-53, *Doctrine for Joint Psychological Operations*. Washington, DC: The Joint Staff, 10 July 1996.
- _____. Joint Publication 3-54, *Joint Doctrine for Operational Security*. Washington, DC: The Joint Staff, 27 January 1997.
- _____. Joint Publication 3-58, *Joint Doctrine for Military Deception*. Washington, DC: The Joint Staff, 31 May 1996.
- Joint Command, Control, and Information School (JCIWS). 2000. *Joint Information Operations Planning Handbook (Second Draft)*. January 2000.
- Koerner, Brendan I. 2000. The Web's Bad Week. *U.S. News & World Report*, 21 February, 19-20.

- Kuehl, Daniel L. 1996. Strategic Information Warfare and Comprehensive Situational Awareness. In *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Fairfax, VA: Armed Forces Communications and Electronics Association International Press.
- Leedy, Paul D. 1989. *Practical Research, Planning and Design*, 4th ed. New York: Macmillan Publishing Company.
- Luvaas, Jay. 1982. Military History: Is it Still Practicable? *Parameters*, March, 2-24.
- Mack, Jennifer. 2000. Attack Victims Count their Losses. *ZDNet News*, 10 February, 1. Available from www.zdnet.com/zdnn/stories/news/0,4586,2436501,00/html
- Marine Corps Combat Development Command. *A Concept for Information Operations*. Quantico, Virginia: United States Marine Corps, 15 May 1998.
- Marine Corps Intelligence Activity. *Marine Corps Midrange Threat Estimate, 1997-2007: Finding Order in Chaos*. Quantico, Virginia: United States Marine Corps, August 1997.
- _____. 1995. *Marine Corps Midrange Threat Estimate 1995-2005*. Quantico, Virginia: United States Marine Corps.
- McConnell, Malcolm. 1991. *Just Cause*. New York: St. Martin's Press.
- Metz, Helen Chapin, ed. 1987. *Libya, a Country Study*. Washington, DC: Federal Research Division, Library of Congress.
- National Security Agency. *Codetalkers Exhibit*. National Cryptologic Museum, March 2000. Available from <http://www.nsa.gov/museum/talkers>. Internet.
- Parker, Robert R., Jr., Major, USMC. 1992. Deception: The Missing Tool. *Marine Corps Gazette*. Quantico, VA: Marine Corps Association, May, 101-102.
- Parks, W. Hays. Colonel, USMCR. 1986. Crossing the Line. *Proceedings*. Annapolis, MD: Naval Institute Press, November, 48.
- Prunckun, Henry W., Jr. 1994. OPERATION EL DORADO CANYON: A Military Solution to the Law Enforcement Problem of Terrorism--A Quantitative Analysis. Thesis submitted to University of South Australia.
- Reuters Newswire. 2000. U.S. Says Cyber-Crime Poses Huge Threat. 16 February, 1.
- Skates, John Ray. 1994. *The Invasion of Japan, Alternative to the Bomb*. Columbia, S.C.: University of South Carolina Press.

- Sniffen, Michael J. 2000. Internet Attacks Extend into this Week and Abroad. *Kansas City Star*, 18 February, 1.
- Summers, Harry G. Jr. Colonel, USA. 1995. *Persian Gulf War Almanac*. New York: Facts on File, Inc.
- Superintendent of Records. 1966. Reports of General MacArthur. *Japanese Operations in the Southwest Pacific Area, Volume II – Part II*. Compiled from Japanese Demobilization Bureau Records. Washington, DC: U.S. Government Printing Office.
- Supreme Commander, Allied Expeditionary Force. 1946. *Report by the Supreme Commander to the Combined Chiefs of Staff on the Operations in Europe of the Allied Expeditionary Force, 6 June 1944 to 8 May 1945*. Washington, DC: U.S. Government Printing Office.
- Trainor, Bernard E. LtGen, USMC. 1986. Deception. *Marine Corps Gazette*, Quantico, VA: Marine Corps Association, October, 57-61.
- Ugaki, Matome. Admiral, Imperial Japanese Navy. 1991. *Fading Victory. The Diary of Admiral Matome Ugaki, 1941-1945*. Translated by Masataka Chihaya. Pittsburgh: University of Pittsburgh Press.
- U.S. Army Special Operations Command, Directorate of History and Museums. *A History of U.S. Army Combat Psychological Operations*.
- U.S. Congress. Subcommittee on Crime of the House Committee on the Judiciary and the Subcommittee on Criminal Justice Oversight of the Senate Committee on the Judiciary. Internet Denial of Service Attacks and the Federal Response. Katherine T. Fithen. Manager, CERT Coordination Center, Software Engineering Institute, Carnegie Mellon University, February 29, 2000.
- U.S. Congress. Senate. Senate Armed Services Committee, Subcommittee on emerging Threats and Capabilities. Cyber Security. Steven E. Cross. Director, Software Engineering Institute, Carnegie Mellon University, March 1, 2000.
- Vander Linde, Dean M. 1987. *Downfall: The American Plans for the Invasion of Japan in World War II*. Thesis submitted to Michigan State University Department of History.
- Venkus, Robert E. Colonel, USAF. 1992. *Raid on Qaddafi*. New York: St. Martin's Paperbacks.
- Warden, John A., III. Colonel, USAF. 1995. The Enemy as a System. *Airpower Journal*, Spring, 40-55.

Wheeler, Richard. 1983. *A Special Valor. The U.S. Marines and the Pacific War*. New York: Harper & Row.

INITIAL DISTRIBUTION LIST

1. Commandant of the Marine Corps
Headquarters, United States Marine Corps
Washington, DC 20380-1775
2. Combined Arms Research Library
U.S. Army Command and General Staff College
250 Gibbon Ave.
Fort Leavenworth, KS 66027-2314
3. Defense Technical Information Center/OCA
8725 John J. Kingman Rd., Suite 944
Fort Belvoir, VA 22060-6218
4. Marine Corps Command and Staff College
Breckenridge Library
MCCDC
Quantico, VA 22134
5. Director
Concepts Development Division
MCCDC
3300 Russell Road
Quantico, VA 22134
6. Director
Doctrine Division
MCCDC C-42
3300 Russell Road, Suite 318A
Quantico, VA 22134
7. Commanding General
MAGTF Staff Training Program
MCCDC C-54
3300 Russell Rd.
Quantico, VA 22134
8. Commanding General
Marine Corps Warfighting Lab (C-52)
3255 Meyers Avenue
Quantico, VA 22134

9. Lieutenant Colonel Frederic W. Lickteig, USMC
Marine Corps Detachment
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352
10. Stephen D. Coats, Ph.D.
Department of Joint and Multinational Operations
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352
11. Lieutenant Commander Gregory M. Landis, USN
Department of Joint and Multinational Operations
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352
12. Colonel Reno C. Bamford, USMC
Marine Corps Detachment
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 4 June 1999
2. Thesis Author: Major Scott D. Aiken, USMC
3. Thesis Title: MAGTF Offensive Information Operations, Supporting Operational Maneuver from the Sea.

4. Thesis Committee Members

Signatures:

[Handwritten signatures: J. W. ...]

[Handwritten signature: Tom ...]

[Handwritten signature: Stephen ...]

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

<u>Limitation Justification Statement</u>	<u>/</u>	<u>Chapter/Section</u>	<u>/</u>	<u>Page(s)</u>
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:

<u>Limitation Justification Statement</u>	<u>/</u>	<u>Chapter/Section</u>	<u>/</u>	<u>Page(s)</u>
_____	/	_____	/	_____
_____	/	_____	/	_____
_____	/	_____	/	_____
_____	/	_____	/	_____
_____	/	_____	/	_____

7. MMAS Thesis Author's Signature: Scott D. Aiken MAJOR, USMC

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).