DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY TRAINING AND DOCTRINE COMMAND
950 JEFFERSON AVENUE
FORT EUSTIS, VIRGINIA 23604-5700

April 21, 2021

Office of the Deputy Chief of Staff, G-6

John Greenewald, Jr.
[redacted]

Dear Mr. Greenewald:

This is in response to your Freedom of Information Act (FOIA) request dated July 3, 2015, to the Defense Technical Information Center for the “(U) Information Operations: A Valid Core Mission for Special Forces”. The FOIA request was referred to the U.S. Army Training and Doctrine Command (TRADOC) and subsequently referred to the U.S. Army Installation Management Command, Fort Leavenworth Garrison, FOIA Office, where it was processed and referred back to TRADOC on December 6, 2017, and assigned control number 18-0030.

As requested, enclosed is the responsive TRADOC record from the U.S. Army Combined Arms Center. Portions of the records have been redacted and the FOIA exemption that prohibits the information disclosure is cited.

FOIA exemption (b)(3) exempts matters from disclosure by statute provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld. 5 U.S.C. § 552(b)(3) implemented by 32 CFR Part 518.13(c). Specific to this request is 10 U.S.C. § 130b, exempts personnel in overseas, sensitive, or routinely deployable units: nondisclosure of personally identifying information.

FOIA exemption (b)(6) protects from release of names and other personally identifiable information pertaining to third parties, especially statements that are unique and specific to small groups of individuals. 5 U.S.C. § 552(b)(6). There is no discretion in release of information that qualifies for withholding pursuant to FOIA exemption (b)(6).

This decision is considered a TRADOC partial denial response to your FOIA request. General Paul E. Funk II, Commanding General, TRADOC, is the Initial Denial Authority (IDA) and by position I am the delegated IDA.

For any further assistance and to discuss any aspect of your request, you may contact the specialist who processed your request, as well as, our TRADOC FOIA

Public Liaison, Mrs. Kakel at (757) 501-6538, or usarmy.jble.tradoc.mbx.hq-tradoc-foia@army.mil. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The OGIS contact information is Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; toll free (877) 684-6448; (202) 471-5770; ogis@nara.gov; or facsimile at (202) 741-5769.

If you are not satisfied with this request response, you may administratively appeal by writing to the **TRADOC FOIA Office** at **U.S. Army Training and Doctrine Command, Office of the G-6 (ATIM), 661 Sheppard Place, Fort Eustis, VA 23604-5733**, and it will be forwarded to the Army General Counsel for final disposition on behalf of the Secretary of the Army. To meet the deadline for the appeal, the appeal letter must be received by this office and forwarded to the Secretary of the Army within ninety (90) days of the date of this partial denial determination response letter.

In your appeal, you must state the basis for your disagreement with the partial denial determination response. Please address your appeal to the **TRADOC FOIA Office**. Please note that your appeal cannot be used to make a new request for new or additional information.

Based on your FOIA request in the media category, there are **no fees assessed** for processing this FOIA request.

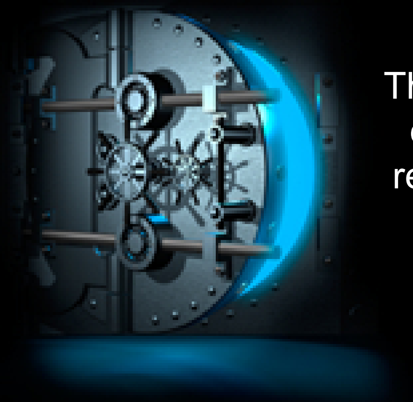
Point of contact is the Government Information Specialist at usarmy.jble.tradoc.mbx.hq-tradoc-foia@army.mil.

Sincerely,

Mark Thomson

Mark A. Thomson
Colonel, U.S. Army

Enclosure



REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE 2 Jun 00	3. REPORT TYPE AND DATES COVERED Master's Thesis 6 Aug 99 - 2 Jun 00

4. TITLE AND SUBTITLE

INFORMATION OPERATIONS: A VALID CORE MISSION FOR SPECIAL FORCES

5. FUNDING NUMBERS

6. AUTHOR(S)

(b) (6)

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

20001115 095

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Distribution authorized to United States (U.S.) Government agencies ~~to protect technical or operational information from dissemination.~~ Administrative or Operational Use , Jun 2000. Other requests to,

12b. DISTRIBUTION CODE

B

13. ABSTRACT (Maximum 200 words)

This study investigates the new Special Forces doctrine that incorporates Information Operations as a core Special Forces mission. It argues whether the inclusion of Information Operations as a core mission is a valid doctrinal change. Because of new technologies and the pervasive integration of computers into everything we do, the Army is looking for how best to synchronize the application of these technologies of massive data collection. New doctrine is being developed to include these technologies. The new joint doctrine for SOF now includes the five stated core missions and adds four more: Psychological Operations (PSYOPs), Civil Affairs (CA), Counterproliferation of weapons of mass destruction (CP) and Information Operations (IO). This study explains why information operations should not be added as a core Special Forces mission. It also examines how Special Forces already contributes to the operational commander's overall Information Operations plan and how Special Forces will continue that contribution in the future. Finally this study recommends the inclusion of new specific skill sets for Special Forces soldiers that are necessary for the XXIst Century.

14. SUBJECT TERMS

Special Forces, Information Operations, Special Operations, Information Warfare, Command and Control Warfare

15. NUMBER OF PAGES

89

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UL

INFORMATION OPERATIONS: A VALID CORE MISSION FOR SPECIAL FORCES

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
General Studies

by

(b) (6) (b) (6) J, (b) (6)
B.S., Middle Tennessee State University, 1988

Fort Leavenworth, Kansas
2000

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of Candidate: (b) (6) [redacted]

Thesis Title: Information Operations: A Special Forces Core Mission?

Approved by:

(b) (6), (b) (6)

(b) (6) (b) (6) [redacted]

(b) (6) (b) (6)

(b) (6) (b) (6)

Accepted this 2d day of June 2000 by:

(b) (6), (b) (6) [redacted]

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

INFORMATION OPERATIONS: A VALID CORE MISSION FOR SPECIAL FORCES by (b) (6) [redacted] [redacted] (b) (6) [redacted] 84 pages.

This study investigates the new Special Forces doctrine that incorporates information operations as a core Special Forces mission. It argues whether the inclusion of information operations as a core mission is a valid doctrinal change.

Because of new technologies and the pervasive integration of computers into everything the Army does, the Army is looking for how best to synchronize the application of these technologies of massive data collection. New doctrine is being developed to include these technologies. Special Forces have traditionally had five core missions. They are Unconventional Warfare (UW), Foreign Internal Defense (FID), Direct Action (DA), Special Reconnaissance (SR), and Combating Terrorism (CT). The new joint doctrine for Special Operation Forces (SOF) now includes the five stated core missions and adds four more: Psychological Operations (PSYOPs), Civil Affairs (CA), Counterproliferation of weapons of mass destruction (CP) and Information Operations (IO).

This study explains why information operations should not be added as a core Special Forces mission. It also examines how Special Forces already contributes to the operational commander's overall information operations plan and how Special Forces will continue that contribution in the future. Finally this study recommends the inclusion of new specific skill sets for Special Forces soldiers that are necessary for the twenty-first Century.

ACKNOWLEDGMENTS

There are too many people to thank here personally; however, I must express my deep gratitude to some of those who made this possible. First, to my family whose support while I retired to "the cave" was immeasurable thank you. Next, I would like to thank my committee, (b) (6) , (b) (6) (b) (6) [redacted], and (b) (6) for their patience, guidance and direction. Finally, to the countless friends and neighbors who endured my tirades about this project thank you for listening.

TABLE OF CONTENTS

FIGURES

TABLES

CHAPTER 1

INTRODUCTION

> Know yourself and know the enemy and in 100 battles you will never fear defeat.
>
> Sun Tzu, *The Art of War*

Information is a part of warfare. Information is the basis from which intelligence is built. It is the cornerstone upon which commanders build decisions. Information has always been required, requested, and even fought and died for in the pursuit of victory on the battlefield. There are many published manuals outlining intelligence, how to collect it, analyze it, and use it. In 1996, the U.S. army published Field Manual (FM) 100-6, *Information Operations*, and in October 1998, Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations* was published. The joint doctrine publication states:

> IO [Information Operations] capitalizes on the growing sophistication, connectivity, and reliance on information technology. IO targets information or information systems in order to affect the information-based process, whether human or automated. Such information dependent processes range from National Command Authorities-level decision making to the automated control of key commercial infrastructures such as telecommunications and electric power. (JP 3-13 1998, vii)

Joint doctrine further defines command and control warfare (C2W) as an application of information operations in military operations that specifically attack and defend the C2 target set. The capabilities and activities employed in C2W are psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, as well as other less traditional methods focused on information systems.

These capabilities can be employed to achieve broader information operation objectives that are outside the command and control target set (JP 3-13 1998, I-4).

Figure 1 gives examples of IO objectives that fall across the three different levels of warfare; strategic, operational and tactical.

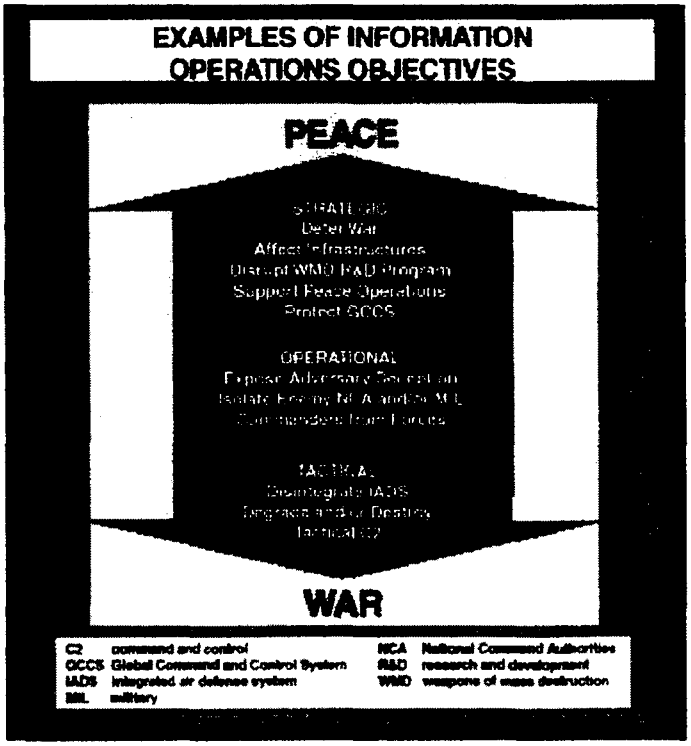

EXAMPLES OF INFORMATION OPERATIONS OBJECTIVES
PEACE
STRATEGIC
Deter War
Affect Infrastructures
Disrupt WMD R&D Program
Support Peace Operations
Protect GCCS
OPERATIONAL
Expose Adversary Deception
Isolate Enemy NCA and/or MIL
Commanders from Forces
TACTICAL
Disintegrate IADS
Degrade and/or Destroy
Tactical C2
WAR
C2 command and control
GCCS Global Command and Control System
IADS integrated air defense system
MIL military
NCA National Command Authorities
R&D research and development
WMD weapons of mass destruction

Figure 1. Examples of IO Objectives. (Source: JP 3-13 1998, II-2.)

Similarly, Special Operations Forces (SOF) are also as old as warfare itself. Current US Special Operations Forces trace their linage to the birth of this nation. One component of SOF, Special Forces (SF), has its genesis rooted in unconventional missions. In fact it has been stated that Special Forces was developed for the purpose of unconventional warfare (UW) (Jones and Tone 1999, 12:3).

In 1969, UW was defined as "military, political, psychological, or economic actions of a covert, clandestine, or overt nature within areas under the actual or potential control or influence of a force or state whose interests and objectives are inimical to those of the United States."(FM 31-21 1969, 3-1). Figure 2 shows notional information operations engagement timelines.

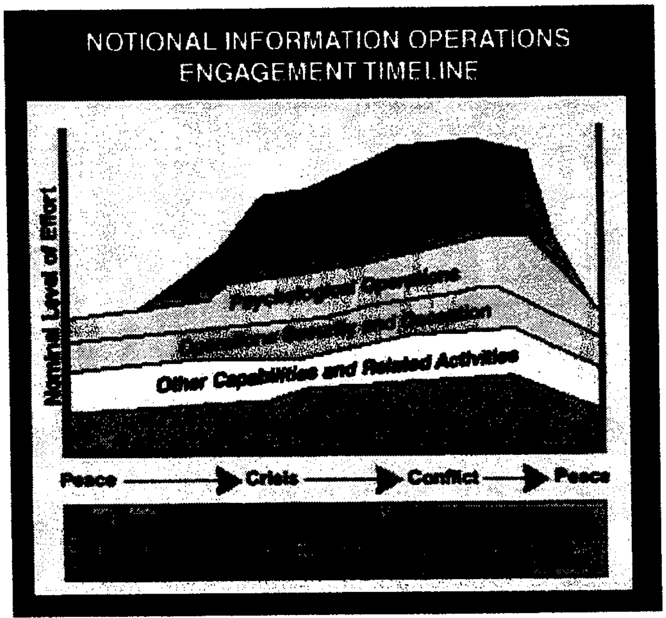
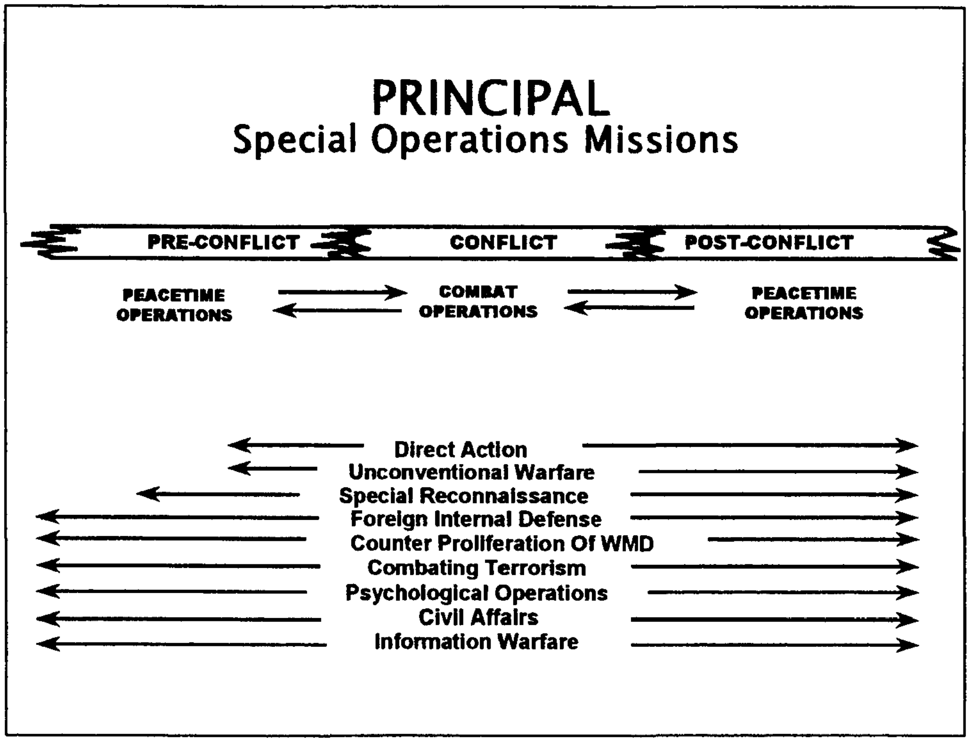


Figure 2. Notional Information Operations Engagement Timeline. (Source: JP 3-13 1998, II-8.)

Figure 3 shows the core Special Forces missions across the operational continuum.



PRINCIPAL
Special Operations Missions

PRE-CONFLICT
CONFLICT
POST-CONFLICT

PEACETIME OPERATIONS
COMBAT OPERATIONS
PEACETIME OPERATIONS

Direct Action
Unconventional Warfare
Special Reconnaissance
Foreign Internal Defense
Counter Proliferation Of WMD
Combating Terrorism
Psychological Operations
Civil Affairs
Information Warfare

Figure 3. Core SOF missions across the Operational Continuum. (Source: SOCOM, Command Brief Slides May 1999.)

Today's modern US Special Forces doctrine is based upon those unconventional roots and further stipulates that specially trained and equipped units accomplish SOF missions (FM 31-20 1998, 1-4). Special Forces has traditionally had five core missions: unconventional warfare (UW), foreign internal defense (FID), direct action (DA), special reconnaissance (SR), and combating terrorism (CT). Recently that changed with the publication of JP

3.05, *Doctrine for Joint Special Operations*, dated April 1998, and FM 100-25, *Doctrine for Army Special Operations Forces (ARSOF) (FINAL DRAFT)*, dated July 1998. These doctrinal manuals state Special Forces now have nine core missions: the five stated above and psychological operations, civil affairs, counterproliferation of weapons of mass destruction and information operations. However, one problem is that joint, Army, and SOF doctrine define what information operations differently.

In the joint doctrine, psychological operations are an integral part of information operations. Psychological operations are actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals (JP 3-13 1998, II-4). This is evidence that at least one component of Special Forces is vested in information operations, that component is psychological operations.

Furthermore, joint doctrine states, "The unique capabilities of SOF enable the Joint Forces Commander (JFC) to access, alter, degrade, delay, disrupt, deny, or destroy adversary information systems throughout the range of military operations and at all levels of war"(JP 3-05 1998, I-17).

To complicate matters the different levels of doctrine, joint, Army and SOF, publish subtly different definitions of information operations. It would appear joint, Army, and SOF doctrine are not adequately nested concerning information operations.

The Research Question

This paper will address this question:

Should Special Forces doctrine expand its core missions?

Assumptions

The following assumptions were made in writing this paper. First, information operations are here to stay. New information operations doctrine lays a foundation to bridge gaps between old technologies and new. The new doctrine will incorporate valid time-tested principles with a variety of rapidly expanding and ever-changing advances in information collection, storage, retrieval and usage.

Definitions

In order to aid with some unique lexicon the following terms have their doctrinal definitions listed in the glossary:

Command and Control Warfare (C2W)

Computer Network Attack (CNA)

Defense Information Infrastructure (DII)

Defensive IO

GII Global Information Infrastructure (GII)

Information

Information Assurance

Information Environment (IE)

Information Operations (IO)

Information Superiority

Information Warfare (IW)

National Information Infrastructure (NII)

Offensive IO

Special Information Operations (SIO)

Special Forces (SF)

Special Operations Forces (SOF)

Special Operations (SO)

Limitations

This paper will be limited in its scope. Information operations doctrine is relatively new and some published material is classified. This thesis is unclassified and therefore will omit classified data or include research that would classify it. This thesis will not look at the areas of psychological operations, civil affairs or public affairs in information operations except to define them in accordance with current doctrine.

Delimitations

This study will limit the scope of research to the impact and relevance of Special Forces conducting offensive information operations and defensive information operations, information warfare, and command and control warfare. It will examine recent and current Special Forces operations defined as information operations missions, excluding those mentioned in the limitations. It will review doctrine published at the joint, Special Operations Command(SOCOM), and Army level.

Significance of the Study

As the twenty-first century begins, the amount of and speed which information is passed and assimilated is rapidly increasing. Due to the introduction of the microprocessor and gains in technology, the United States' enemies are leveraging new technologies in an effort to defeat it not only on the battlefield but also with asymmetrical means. Because of this, the Army is looking at new and innovative ways to remain dominant and to protect its national security interests. Special Forces have always been at the tip of the spear in meeting those adversaries and will continue to do so in the foreseeable future.

By approaching these challenges with the same resolve as in the past, Special Forces can help maintain the United States' dominance. A thorough examination of Special Forces' role can determine its relevance in future missions in this dynamic arena and insure its potential is maximized.

Lastly, the Army can ensure Special Forces doctrine captures and reinforces the fundamental principles that outline the creation of the techniques, tactics, and procedures used during mission execution.

Organizational and Methodology

This study consists of five chapters. Chapter 1 is the introduction. It defines the questions and problems and states the significance and parameters of the study.

Chapter 2 contains a review of the literature of books, doctrinal manuals, periodicals, professional journals, unclassified documents published and internet related sites.

Chapter 3 covers the methodology. It examines doctrine, missions, capabilities, equipment, training, and resources. The following methodology is employed:

1. A thorough survey of the literature and analysis of different concepts of information operations.

2. Review current joint and service doctrine, policy, and guidance on information operations and Special Forces.

3. Review the integration of Special Forces and infopmation operations.

4. Examine the types of operations in which Special Forces and information operations are being used together.

5. Examine past roles and missions of Special Forces and inductively extrapolate possible future missions.

Chapter 4 is an analysis of the doctrine comparable to the current and future missions, capabilities, equipment, training, and resources.

Finally, chapter 5 draws conclusions and makes recommendations based on the previous chapters' analysis.

CHAPTER 2

LITERATURE REVIEW

> You must have absolute command of your data above all else. DOD *The Armed Forces Officer* 1975, 103

This chapter covers four areas. First, it looks at past, current, and evolving doctrine regarding both Special Forces and information operations. Second it will review not only the Army doctrine but also joint and other service doctrine. Third, it will review a sampling of publications and books on the past, current, and projected views of information operations and Special Forces. Finally, it will review the information available on the Internet and from formal and informal briefings.

The primary research facility used is the Combined Arms Research Library at Fort Leavenworth, Kansas. Other methods of research include course material found in the Information Operations Course taught by (b) (6) (b) (6) at the Command and General Staff College, Fort Leavenworth, Kansas; briefings and interviews by subject matter experts; and finally information available on the internet posted on official and unofficial websites and file transfer protocols.

The focus of thesis is on Special Forces and information operations at the operational level of war. However, some research will also cover operations at the tactical and strategic levels due to the broad implications of information operations and the span of Special Forces missions across the operational continuum.

Information Operations Doctrinal Publications

It was not until 1996 that the United States Army published FM 100-6, *Information Operations*, and not until October 1998, that JP 3-13, *Joint Doctrine for Information Operations*, was published. It would seem logical that the joint doctrine would be the first published manuscript and from that document the services would derive their doctrine so as to ensure the proper nesting and linkage. It is obvious the different levels of doctrine specify subtly different Information Operations definitions. Even Special Forces doctrine defines information operations differently. Although only three years old, a new Army FM 100-6 is currently being written.

The new manuals attempt to correct these disconnects between joint and Army doctrine and ensure the proper nesting and linkage. The draft version of FM 100-6, *Information Operations: Tactics, Techniques, and Procedures*

(Initial Draft), dated 30 April 1999, breaks down information operations into two categories. They are offensive information operations and defensive information operations. Defined, offensive information operations are the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers or to achieve or promote specific objectives. Defensive information operations are the integration and coordination of policies and procedures, operations, personnel, and technology to protect friendly information and information systems. The new doctrine also establishes an information operations section on the corps and division headquarters' staff headed by an information operations coordinator (IOCORD). The IOCORD is similar to the fire support coordinator (FSCORD). The new doctrine also defines the duties and responsibilities of those new staff members.

With respect to the military's existence and its propensity to regulate, catalog, or incorporate some doctrinal label to everything within its purview, information operations is presented as a new concept, and as mentioned earlier prior to 1996 there was no formal doctrine. However, the new doctrine categorizes some more familiar concepts under the information operations umbrella. Specifically operational security, psychological operations, public affairs operations and military deception, which are not new concepts to the military and on which there are volumes of doctrine and historical writings, are now fully under the umbrella of information operations doctrine. Similarly, information operations include the areas of civil affairs and electronic warfare, which are relatively new to warfare in that, they have only been around for about one hundred years. The current doctrine takes into account the changing nature of warfare and incorporates information operations not only in the narrow operational spectrum of war but also in the broader context of military operations other than war and in peace. Furthermore, it looks at enemy capabilities categorized as asymmetrical threats or those threats that are considered to be nontraditional and transnational and that include information operations.

Based on the joint publications, the Navy and Air Force are now publishing doctrine that incorporates information operations. The Air Force has even published Air Force Doctrine Document 2-5 (AFDD 2-5), *Information Operations;* and AFDD-1, *Air Force Basic Doctrine,* states one of the air and space power functions is counterinformation. According to AFDD 1, "Counterinformation creates an environment where friendly forces can conduct operations without suffering substantial losses, while simultaneously denying the enemy the ability to conduct their operations" (1997, 53)

Special Forces Doctrinal Publications

> There is another type of warfare new in its intensity, ancient in its origin war by guerrillas, subversives, insurgents, assassins; war by ambush instead of combat, by infiltration instead of aggression, seeking victory by eroding and exhausting the enemy instead of engaging him. . . . It preys on unrest.
>
> President John F. Kennedy, January 1961

It is the change in the doctrine of Special Forces, which prompts this thesis. Special Forces doctrine in this country is relatively new in that the first manual was published in the 1950s, compared to the first engineer and artillery doctrine, which was written nearly 200 years ago. Special Forces doctrine has always addressed military operations other than war although during Special Forces' infancy those operations were referred to as low-intensity conflicts. With its roots in what was called guerilla warfare and labeled today as unconventional warfare, the fundamental tactics of Special Forces doctrine based on small groups of specially trained men is still the basis today. Current Special Forces doctrine also takes into account the nontraditional, transnational and asymmetrical threats.

With the evolution and growth of Special Forces, Congress codified in law under United States Code Title 10 the establishment of an overall commander for Special Operations Forces of which Special Forces is a part. That commander is the Commander in Chief for the United States Special Operations Command (USSOCOM) and is responsible for and shall have the authority to develop strategy, doctrine, and tactics (United States Code, Title 10, section 167).

As stated in chapter 1, previously Special Forces had the five core missions: unconventional warfare, foreign internal defense, direct action, special reconnaissance, and combating terrorism. New SOF doctrine in FM 100-25, *Doctrine for Army Special Operations Forces (Final Draft)*, dated July 1998, also includes information operations and counterproliferation of weapons of mass destruction as new missions. Also, the new FM 31-20, *Doctrine For Army Special Forces Operations (Initial Draft)*, dated December 1998 nests the two new missions. The Army SOF publication defines information operations verbatim from the joint publication and adequately explains it in one and one half pages. However, the draft Special Forces field manual allocates ten lines to information operations and uses half of those to define it and example how a direct action mission might be a way to "achieve IO initiatives." The new Special Forces doctrine also states that information operations is "sometimes called Information Warfare (IW)" and "command and control warfare (C2W)." The joint doctrine states that information warfare is "IO conducted during time of crisis or conflict (including war)." Furthermore, the joint publication clearly stipulates C2W as an "application of IO." There are minor examples of nuances and differences between the different levels of doctrines. The Special Forces doctrine does incorporate the doctrinal information operations terminology of both the joint and new Army publications. However, the inclusion of both terminologies is not as effective as it could be, although it does appear to be nested.

Information Operations Publications

There are a growing number of articles and books on information operations. Writings date back to ancient China and Sun Tzu's arcane transcripts in *The Art of War* and include classics, such as Clauswitz's *On War*, as well as more obscure manuscripts like Colonel George Armand Furse's *Information in War: Its Acquisition and Transmission.* Today there is a boom market in books about information operations and the information age. In fact, Dan Kuehl of the National Defense University states, "Anybody who makes more than $5 an hour and works on this side of the Mississippi has tried to define Information Warfare" (Mitchell 1999, 37).

There is a resonating mantra that this is indeed a new age, the information age. Lieutenant Colonel Robert R. Leonhard, author of *The Principles of War for the Information Age,* advocates that some familiar characteristics of warfare have changed and therefore some underlying principles must also change. The author of *Breaking the Phalanx: A New Design for Landpower in the 21st Century* Colonel Douglas A. Macgregor, states that the U.S. Army is experiencing a "revolution in military affairs (RMA)" and has even titled one of his chapters "Fighting with the Information Age Army in the Year 2003."

There are many books that deal specifically with computer attacks and the use of what is widely known as cyberspace to base their research. Cliff Stoll, a Lawrence Berkeley Lab astronomer, chronicled his real-life adventure tracking a hacker breaking into the U.S. computer systems and stealing sensitive military and security information in his book, *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* The book *The Next War: Computers are the Weapons and the Front Line is Everywhere* by James Adams and *The Future of War: Power, Technology and American World Dominance in the 21st Century* by George and Meredith Friedman analyze the effects of new technology. These books look specifically within the world of microprocessors and how they may be employed in warfare in years to come.

There are numerous other books and articles relating to the information age that do not directly relate to the military, but provide insight to the asymmetrical threats currently presented as probable threats to the United States.

Some information operations writings are so forward thinking in their presentation that they are more into the science fiction than the science fact realm of research. However, there is a solid foundation of knowledge from which to draw sufficient data to intelligently extrapolate conclusions on current trends, future possibilities, and speculative probabilities.

Special Forces Publications

There are many books published about Special Forces. They are important because they identify the uniqueness of Special Forces. Furthermore, with the resurgence of Special Forces in the 1980s and 1990s, there is a growing body of work specifically about Special Forces from which to draw. These articles capture current trends and identify the future tendencies of Special Forces.

Publications, such as *Special Operations in U.S. Strategy*, edited by Frank R. Barnett, B. Hugh Tovar, and Richard H. Shultz, combine a variety of papers and look at not only the resurgence of Special Operations Forces and Special Forces but also the need for Special Forces. Doug C. Waller's book *The Commandos: The Inside Story of Americas Secret Soldiers* tells of SOF missions to include Special Forces missions conducted during the Gulf War. (b) (6) [redacted] (b) (6) thesis "Strategic Leverage: Information Operations and Special Operations Forces" is one look to combine the subjects of information operations and Special Forces.

From these magazine articles and books, there is enough information to identify Special Forces' past, and where Special Forces is today and to have a clear picture of where Special Forces is heading in this ambiguous world of asymmetrical enemies, constrained resources, and nebulous missions.

Internet and Briefing Sources

In the world today there is an abundant amount of information at the world's fingertips through the internet. Literally millions of books, articles, and publications are available at the touch of a button. It is one of the easiest and most convenient ways to conduct research and a rich source for freethinking unencumbered analysis usually associated with institutionalized research documents. However, as easy as it is to download text, pictures, and graphics it is just as easy for anyone who owns a computer and "makes more than $5 an hour" can post his views on information operations, information warfare, Special Forces or the future of warfare onto a website and proclaim himself the expert in a matter of mere minutes.

In the same light there are abundant briefings, handouts, slideshows, and other pertinent information relative to this topic. When possible, attempts to interview the briefer or author of the presentation have been made.

So while some literature is downloaded directly from the Internet and taken from presentations, it is understood that the responsibility to ensure the validity of that information is incumbent upon this author.

Conclusion

There is wealth of published literature both on information operations and Special Forces. Clearly there is enough information to provide research and source material to complete this project. The literature is sufficiently comprehensive and with a thorough analysis will provide a foundation to build logical and cogent conclusions regarding information operations and Special forces.

CHAPTER 3

METHODOLOGY

> The military mind always imagines that the next war will be on the same lines as the last. That never has been the case and never will be.
>
> Marshal Ferdinand Foch,
> *The Principles of War*

> Officers no longer look upon history as a kind of dust heap....They go to as a mine of experience where alone the gold is to be found, from which right doctrine the soul of war-can be built up.
>
> Julian Corbett,
> *Some Principles of Maritime Strategy*

Taking exception to Marshal Foch, this thesis will travel down Mr. Corbett's path searching for the gold and take an in-depth look at past and current doctrine, missions, capabilities, training, and resources of information operations and Special Forces. It will examine past and current information operations and Special Forces integration within the confines of unclassified material. This chapter sets the stage for chapter 4. It will analyze inductively extrapolated future information operations missions that could be conducted by Special Force. It will also analyze future Special Forces missions that could be considered as information operations missions.

It shall use the analytical method Known-Unknown-Presumed/Likeness-Differences (K-U-P/L-D) method as defined in *Thinking in Time: The Uses of History for Decision Makers* by Richard E. Neustadt and Ernst R. May. First, it will define what is known (current doctrine and past missions) from what is unclear and what is presumed (future missions and capabilities). Next comparisons of the likeness and differences will be made. Finally, it will analyze the outcome and identify recommendations (Neustadt 1986, 273.)

Information Operations

To begin it is essential to identify past and current information operations. Some authors proclaim the Gulf War of 1991, Desert Shield and Desert Storm, to be the de facto first "information war" because it marked the initial departure from the "mass-based warfare" which had been dominant since the industrial revolution, or because of the use of precision guided munitions and advanced communications (Toffler and Toffler 1993, 76-77). Others go back to the 1989 invasion of Panama, Operation Just Cause, as an info War.

Information transmission and reception has increased throughout the history. From the runners at Marathon to the instant telecommunications in use today, the world has found more effective and efficient means to collect, transmit, and store information. Figure 4 shows the increase in information access over the last 700 yrs.

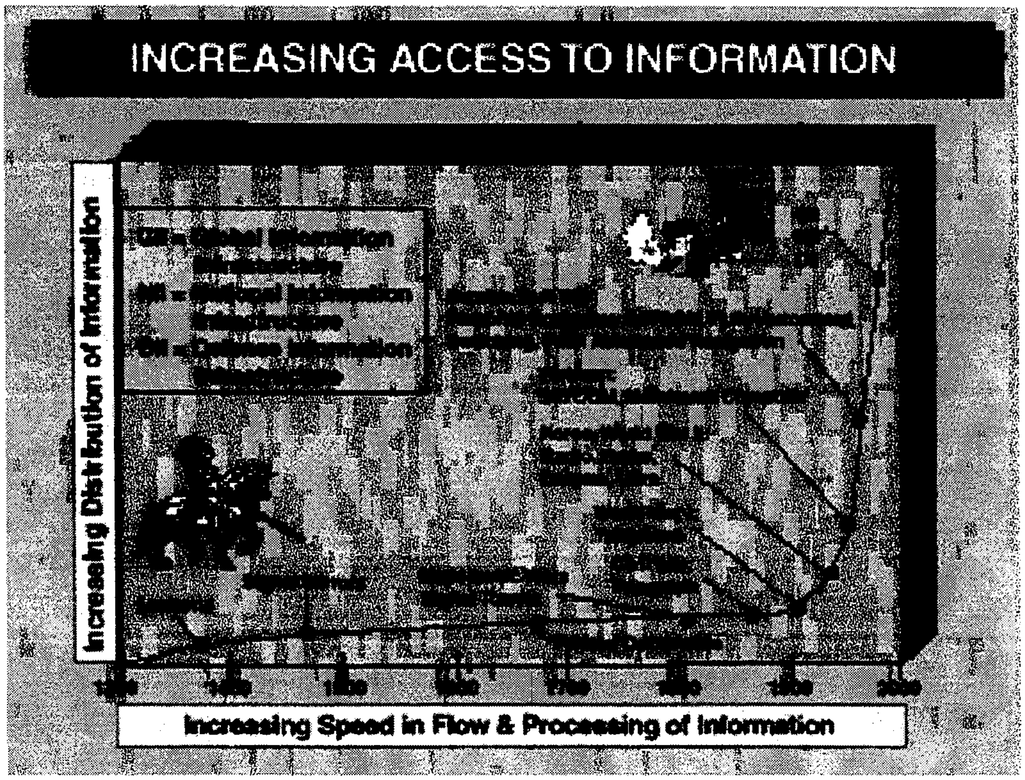


Figure 4. Increasing Access to Information. (Source: JP 3-13 1998, I-12.)

However, because of the broad brush with which information operations doctrine paints with, this thesis will look further back in history. In 1895, Colonel George Armand Furse, CB states, "The information which a commander needs can be divided into two parts-- one that embraces *everything* which refers to the *adversary's* strength, distribution and location, the other to the condition of *his army*"(emphasis added)(Furse 1895, 22). In the definition in chapter 1, current doctrine identifies information as "facts, data, or instructions in any medium or form," and information operations are "action(s) taken to affect *adversary* information and information systems *while defending one's own* information and information systems" (emphasis added)(JP 3-13 1998, I-9). Today's information operations split into two categories, "offensive IO" used "to *affect adversary* decision makers" and "defensive IO" used "*to protect friendly* information."

Colonel Furse goes on to note that "documents, ordinances, notices, telegrams, newspapers, letters-- in short, any printed or manuscript matter found in the enemy's country, may contain valuable information," consequently soldiers must "be instructed to attach great importance to their seizure." In fact, in 1806 "Napoleon instructed Marshal Berthier to solicit the King of Bavaria to have all the letters arriving at Augsberg and Nuremberg from Prussia seized and opened." Not to be outdone Berthier learned in a letter to him that, "the Berlin cabinet has ordered the director of post to stop all letters directed to places which are occupied by the French Army" (Furse 1895, 146).

Colonel Furse further advocates, "relevant items of information can be attained by seizing the office copies of telegrams and at times by tapping the enemy's wires." However, he cautions that the telegraphists be "furnished with [the} proper instruments" (Furse 1895, 148).

Similarly today adversaries have obtained "relevant items of information" through computer systems. In one case, a technician trying to track a computer intruder watched as a secret document from a naval facility was "hijacked" from the computer system. Hackers entered the system through an overseas site on the Internet. It is suspected that several other intrusions had gone undetected. Oleg Kalugin, a former head of Soviet counterintelligence now resident in Maryland, said "Such facilities were prime targets for Russian intelligence." Moscow Internet servers were used to gain access in some attacks. Russia is pressing for an international treaty to freeze information warfare. "We cannot permit the emergence of a fundamentally new area of international confrontation," Sergei Ivanov, the former Russian foreign minister, wrote in a letter to Kofi Annan, the United

Nations secretary-general in October. (Campbell, 1999). Ironically the Russians have publicly talked about using nuclear weapons in response to an information attack (Thomas 1996, 26).

These are but two examples of information acquisition one past and one present. Colonel Furse lists 12 methods for obtaining information in the field in 1895:

1. Through the cavalry which covers the army
2. Through reconnaissance
3. By judicious employment of spies
4. By questioning prisoners and deserters
5. By details furnished by scouts or patrols
6. By particulars acquired by the military police
7. From newspaper reports
8. By tapping the enemy's telegraph wires, or by seizing originals or copies of telegrams
9. By intercepting couriers or other individuals bearing dispatches
10. By seizing correspondence passing through the post, documents found on prisoners, amongst the effects of the enemy's dead, or in offices, hotels, or private dwellings
11. By questioning the inhabitants

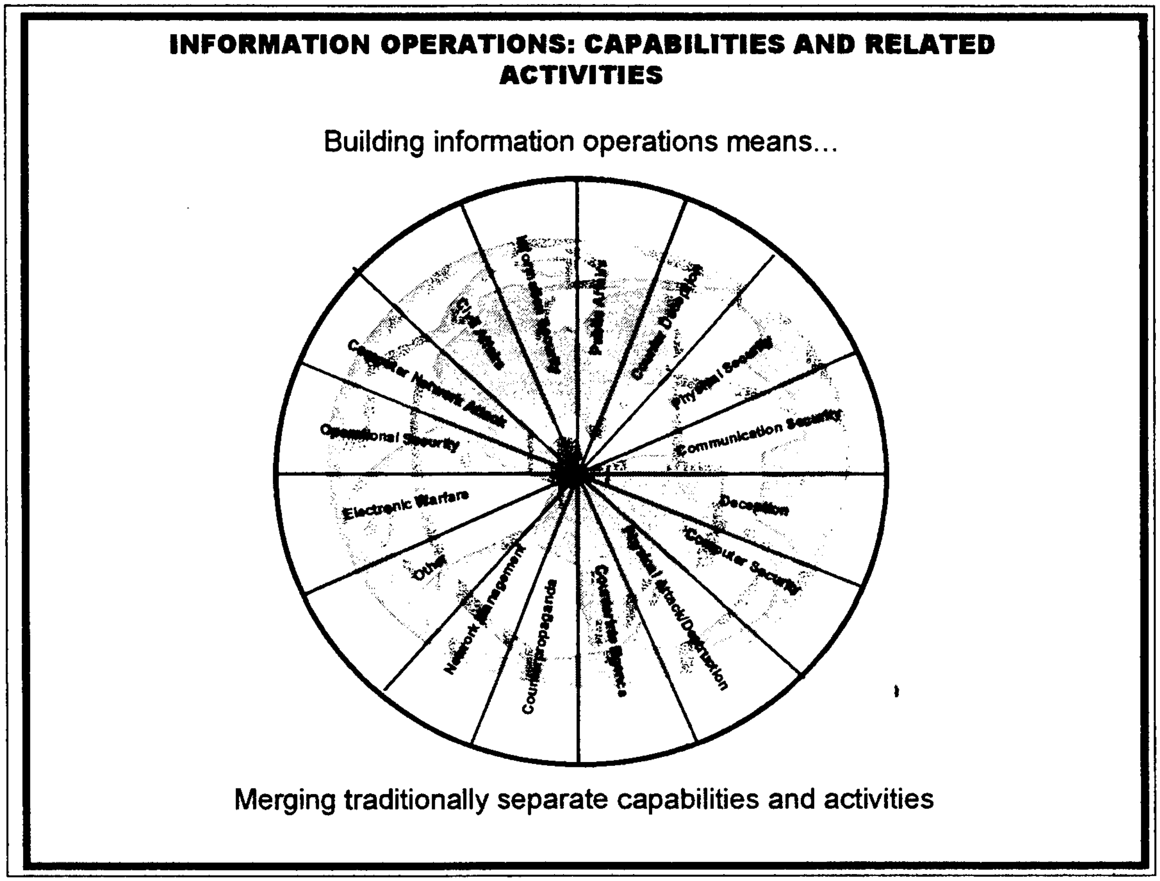
12. From certain special indications. (Furse 1895, 27)

Today current IO doctrine merges traditionally separate capabilities and activities. As mentioned earlier, the doctrine identifies two parts that those capabilities and activities fall under offensive information operations and defensive information operations. Table 1 and figure 5 show the subcategories of both of these types of information operations.

OFFENSIVE IO	DEFENSIVE IO
Operations Security	Operations Security
Military Deception	Counterdeception
Psychological Operations	Counter-Propaganda
Electronic Warfare	Electronic Warfare
Physical Attack/Destruction	Physical Security
Special IO	Counterintelligence
Computer Network Attack	Computer Network Defense
Public Affairs	Public Affairs
Civil Affairs	Command Information

Table 1. Offensive and Defensive Assigned and Supporting IO Capabilities and Activities. (Source: JP

It is interesting to note that some of the same methods employed one-hundred years ago are still used today even though it is claimed the Army is in the advent of a Revolution in Military (RMA) brought upon the it by information operations. Although in 1895 the terminology was not coaxed in catchy little buzzwords and mnemonic phrases that is common today. .



INFORMATION OPERATIONS: CAPABILITIES AND RELATED ACTIVITIES

Building information operations means...

Merging traditionally separate capabilities and activities

Figure 5. Assigned and Supporting IO Capabilities and Activities. (Source: JP 3-13 1998 I-10.)

The new information operations doctrine also establishes an IO section at the corps and division level headed by an IOCORD. This IOCORD is similar to the FSCORD already on the staff. This information operations coordinator will be a school trained in the new career field designator (CFD) 30, Information Operations.

According to the draft FM 100-6, *Information Operations*, the information operations staff is to be a "combat multiplier for the commander" and conducts normal staff responsibilities as outlined in FM 101-5, *Staff Organization and Operations*, as well as information operations specific actions, such as:

1. Establish IO priorities to accomplish planned objectives
2. Synchronize the effects of offensive and defensive IO
3. Coordinate within the staff the various forms of offensive and defensive IO
4. Deconflict offensive and defensive IO to support the commander's concept of the operation through the planning process
5. Recommend to the G3 taskings for the assets needed to execute IO
6. Coordinate IO input into the commander's guidance, concept of operation and coordinating instructions
7. Coordinate intelligence support from the ACE, national level assets, and Special Technical Operations (STO)
8. Assess the impact of offensive and defensive IO into information operations to create a common operational picture for the commander

9. Ensure solutions are provided to the command to reverse IO vulnerabilities (FM 100-6 1999, 2-3).

The draft document also envisions the IO staff to be seventeen personnel at the Corp level.

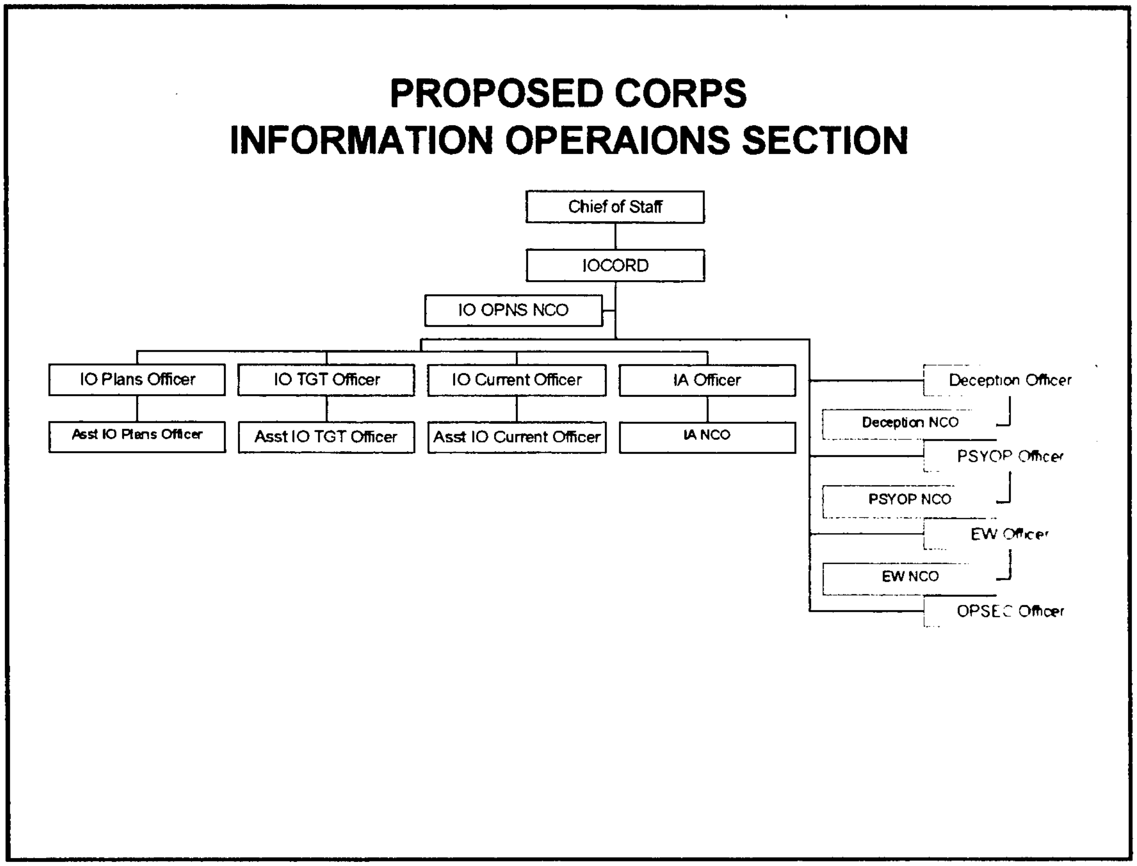


Figure 6. Proposed Corp Staff IO Section (Source: FM 100-6 1999, 2-4.)

As was pointed out in chapter 2, the new doctrine categorizes some more familiar concepts under the IO umbrella. Operational security, psychological operations, public affairs operations and military deception are not new concepts to the military. However, these are now tenants fully under the umbrella of IO doctrine. Similarly information operations now include civil affairs and electronic warfare. Information operations also look at enemy capabilities categorized as asymmetrical threats or those threats considered to be nontraditional, transnational.

Asymmetrical warfare can best be defined as indirect warfare. This type of warfare is familiar to the unconventional warrior or guerrilla fighter. Today's terrorism is the best example of a type of asymmetrical warfare. By methods, such as kidnapping, and bombings of cultural and civilian centers, these terrorists hope to leverage public outrage over real or perceived injustices to bring about political change. One example of this type of warfare includes the suicide truck bomber that provided the catalyst for the U.S. withdrawal of Lebanon in 1983. Today the Hezballah uses bombings, ambushes, and targeted television broadcasts of those events into Israel to bring about the Israeli withdrawal out of southern Lebanon. One final example of asymmetrical warfare would be the kidnapping or death of a key individual or a few selected individuals responsible for integrating or planning of complex systems. By eliminating these key people, the second order effect is in essence to shut down the system or degrade its capability.

It will be interesting to see the new information operations doctrine at work within the joint arena. A joint task force (JTF) will have a psychological operations staff officer under the IOCORD in the JTF's IO section and a joint psychological operation task force (JPOTF) Commander who will command the JTF's psychological operations forces.

In that joint task force, there will be another subordinate commander the Joint Special Operations Task Force Commander (JSOTF). He will command the Special Operations Forces, which include Special Forces. Figure 8 shows the C2 and liaison for the joint task force Special Operations Forces. Figures 7 and 8 illustrate examples of a typical joint information operations cell and a Special Operations Forces subordinate joint force command and control and liaison.

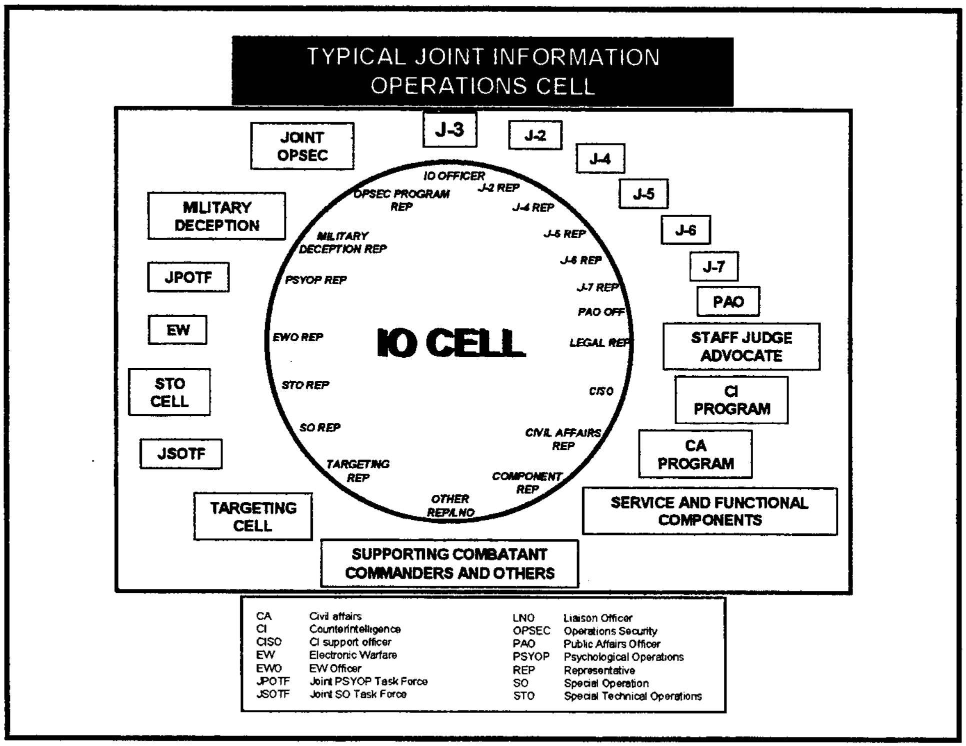


Figure 7. Typical Joint Information Operations Cell. (Source: JP 3-13 1998, IV-3.)

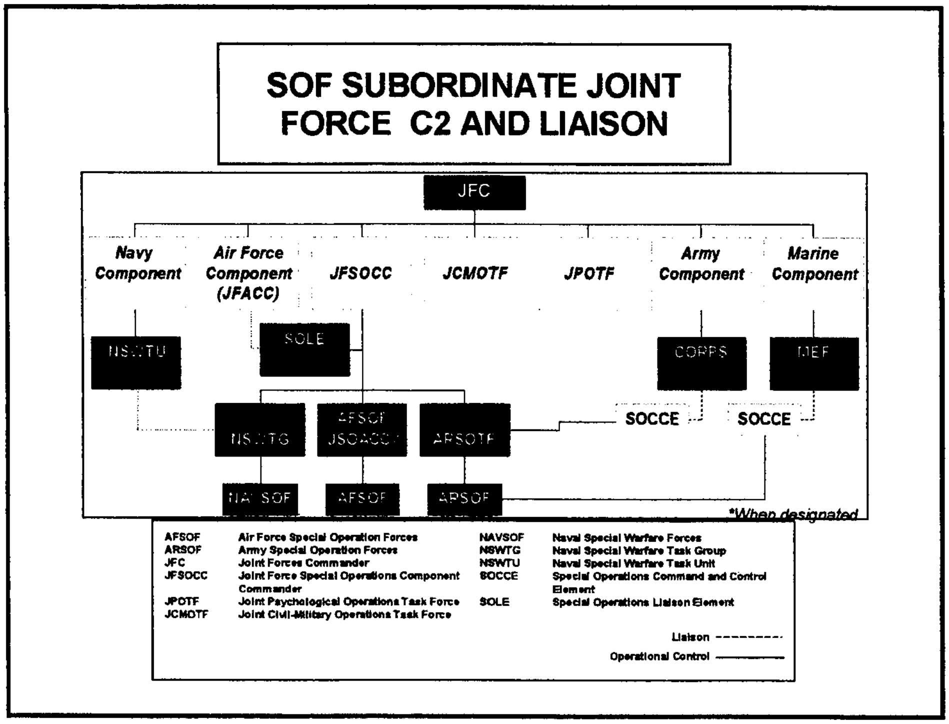

SOF SUBORDINATE JOINT FORCE C2 AND LIAISON
JFC
Navy Component
Air Force Component (JFACC)
JFSOCC
JCMOTF
JPOTF
Army Component
Marine Component
NSWTU
SOLE
CORPS
MEF
NSWTG
AFSOF JSOACC*
ARSOTF
SOCCE
SOCCE
NAVSOF
AFSOF
ARSOF
*When designated
AFSOF Air Force Special Operation Forces
ARSOF Army Special Operation Forces
JFC Joint Forces Commander
JFSOCC Joint Force Special Operations Component Commander
JPOTF Joint Psychological Operations Task Force
JCMOTF Joint Civil-Military Operations Task Force
NAVSOF Naval Special Warfare Forces
NSWTG Naval Special Warfare Task Group
NSWTU Naval Special Warfare Task Unit
SOCCE Special Operations Command and Control Element
SOLE Special Operations Liaison Element
Liaison
Operational Control

Figure 8. SOF Subordinate Joint Force C2 and Liaison. (Source: JP 3-05 1998, III-4.)

Next this thesis will discuss past and current Special Forces doctrine and missions.

Special Forces

> The demands of SO require forces with attributes that distinguish them from conventional forces.
> (JP 3-05 1998, *Doctrine for Joint Special Operations,* II-2*)*

Having previously highlighted the five core missions of Special Forces, the next portion will take a brief look at four of those missions: unconventional warfare, direct action, foreign internal defense, and special reconnaissance. Each mission is covered in a different period of time over the last fifty years. Unconventional warfare is viewed from during World War II. Direct action is exampled during the Vietnam War and the Gulf War. Foreign internal defense is viewed from the 1980s fight in El Salvador at the end of the cold war. Finally special reconnaissance is looked at from Desert Sword in 1991. The intention is to give a sampling of Special Forces missions over a wide swath of modern history. It is intended only to summarize briefly the uniquely diverse capabilities Special Forces have had and continue to possess.

Modern day Special Forces soldiers trace their lineage to the legendary beginnings of the Office of Strategic

Services (OSS) and Colonel Aaron Banks of the infamous Jedburgh Teams. The Jedburghs were three-man teams who parachuted into axis-occupied France before, during, and after the allied assault into France on 4 June 1944. These teams armed and trained the Maquis, the French resistance. (Brown 1982, 525). By August 1944 the Jedburghs were in command of over 30,000 armed maquisards (Brown 1982 571).

Activated in June 1952, the 10th Special Forces Group consisted of seven enlisted men and one warrant officer and one colonel, Colonel Aaron Bank (Paddock 1999, 8). From this auspicious beginning, today there are five active duty and two National Guard Special Forces Groups consisting of approximately 4100 Special Forces qualified soldiers and an additional 4000 soldiers supporting them (Ashley 2000).

After World War II and during the cold war with the former Soviet Union, the need of a force to train an indigenous resistance like the Jedburghs, drove the development of the organization of the Special Forces alpha detachments or A-Teams. These teams consisted of thirteen noncommissioned officers, a captain commanding and a first-lieutenant executive officer. These teams were able to infiltrate behind enemy lines and organize, train, and direct friendly forces in a guerilla war (Paddock 1999, 8).

Today's Special Forces Organization

Today Special Forces Operational Detachment Alphas (SFODAs) are similarly organized. Commanded by a captain, the team also has a warrant officer as the assistant detachment commander. The senior enlisted member of the team is a master sergeant. He is usually referred to as the team sergeant. Next in the chain of command is the operations and intelligence sergeant. He is usually the senior sergeant first class on the team. Rounding out the team are the men filling the team's weapons, engineer, communications, and medical positions. Each of those specialties has two noncommissioned officers one in a senior role and the other in a junior role. These twelve men constitute the modern day Special Forces A-team. Besides the basic skills mentioned above they can also bring a variety of other skills, such as sniper training, advanced demolitions, advanced special operations techniques (ASOT). Also the team members may be trained in a specialized infiltration method, such as military freefall (MFF) or self-contained underwater breathing apparatus (SCUBA).

Figure 9 depicts a typical Special Forces Operational Detachment A.

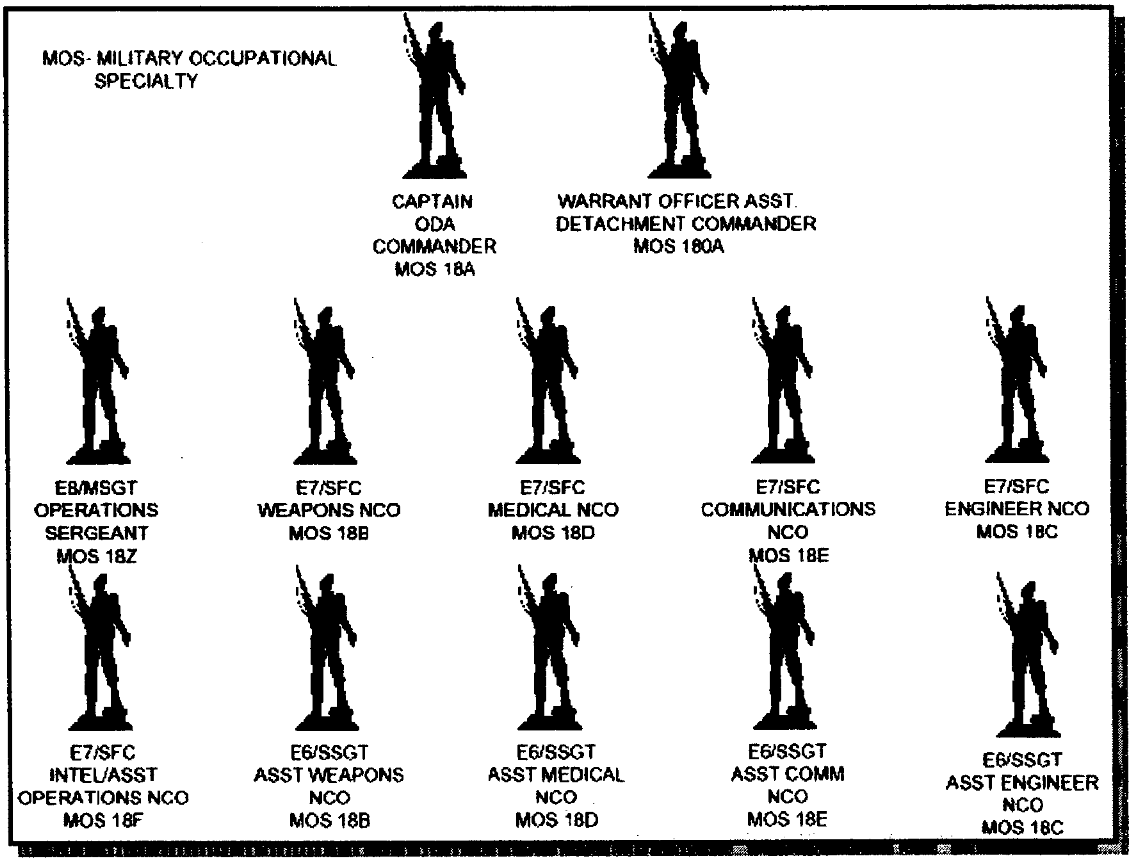

MOS- MILITARY OCCUPATIONAL SPECIALTY
CAPTAIN ODA COMMANDER MOS 18A
WARRANT OFFICER ASST. DETACHMENT COMMANDER MOS 180A
E8/MSGT OPERATIONS SERGEANT MOS 18Z
E7/SFC WEAPONS NCO MOS 18B
E7/SFC MEDICAL NCO MOS 18D
E7/SFC COMMUNICATIONS NCO MOS 18E
E7/SFC ENGINEER NCO MOS 18C
E7/SFC INTEL/ASST OPERATIONS NCO MOS 18F
E6/SSGT ASST WEAPONS NCO MOS 18B
E6/SSGT ASST MEDICAL NCO MOS 18D
E6/SSGT ASST COMM NCO MOS 18E
E6/SSGT ASST ENGINEER NCO MOS 18C

Figure 9. Special Forces Operational Detachment Alpha organization. (Source: SOCOM 1998, 3-16.)

The fundamental tactics of Special Forces doctrine are based on small groups of specially trained men. It was these tactics that the Kennedy and Johnson administrations saw as the way to combat the communist threat in Indochina in the early 1960s. These teams were originally designed to fight behind soviet lines when they began their rush to conquer Europe. Now they would be used to train the South

Vietnamese Army and its people how to defend themselves from the onslaught of communist aggression from the North.

It was from these teams that men were called upon to perform other missions. During Viet Nam, Special Forces teams conducted long-range reconnaissance missions for operational and strategic objectives. Special Forces teams also conducted raids and ambushes. Probably the most famous of these and unquestionably the most publicized was the raid on the Son Tay prisoner of war camp.

Led by Colonel Arthur "Bull" Simmons, this direct action mission was characterized by many trademark Special Forces principles. It was a strategic raid approved by the National Command Authority. It used specialized equipment, was a joint operation incorporating 105 aircraft for the entire operation and required very detailed planning.

The planning began in August 1970 and rehearsals began soon after that. An exact scale model of the compound was made and is on exhibit today in the Special Forces Museum at Fort Bragg, North Carolina. Also a full-scale replica of the compound was built in Florida for the rehearsals. This compound was built daily and dismantled to avoid detection by Soviet reconnaissance satellites passing overhead. This is an indicator of the level of operational security built into the plan. President Nixon gave approval for a 21 to 24 November raid that was moved up to 20 November due to weather considerations. Although the raid failed to rescue any POWs, it completely surprised the North Vietnamese and resulted in over one hundred enemy killed and wounded with no US killed and only two minor casualties (DOD 1999).

Special Forces were once again used to combat counterinsurgency in a foreign internal defense role in the 1980s in El Salvador. Special Forces worked directly with El Salvadoran counterparts and laid the groundwork for the defeat of the communist Farabundo Marti Liberation Front resulting in the signing of the peace accords in 1992. So successful were the operations that the government forces and rebels both insisted that Special Operations Forces play a role in the disarmament and demobilization of combatants that ended the war. This success has made a significant contribution to the overall peace in Latin America (JP 3-05 1998, II-7).

Figure 10. Special Forces conducting special reconnaissance deep inside Iraqi territory during operation Desert Storm. (Source: SOCOM Pub 1, 1998, 30.)

In DESERT SHIELD and DESERT STORM Special Forces performed special reconnaissance missions acting as forward scouts for General Norman Schwarzkopf the theater commander in chief (CINC). Some teams were camped along the northern Saudi border, reported Iraqi troop movements and served to warn the CINC if the Iraqis moved south (Waller 1994, 291). Other missions provided operational intelligence for General Schwarzkopf in executing the "Hail Mary" turning movement. The teams provided valuable human intelligence (HUMIT) with eyes-on reconnaissance and were positioned to monitor enemy troop movements. The information allowed the VII Corps commander to move freely his units without fear of being flanked by the Iraqi Republican Guard (FM 100-25 1999, 2-8).

One DA mission sent a 6-man Special Forces team with a British SAS element to cut a fiber optic cable that stretched from Baghdad to southwest Iraq believed to be part of the C2 architect for that sectors Air Defense (Waller 1994, 359). Another DA mission constituted the "recapture" of the American Embassy in Kuwait (Waller 1994, 293).

The DESERT STORM missions are characterized in today's doctrine as not only special reconnaissance and direct action but as information operations. Specifically, the special reconnaissance missions were information operations because they were a "key role in intelligence preparation of the battle space (IPB)." The fiber-optic DA mission helped "shape the adversary's C2" (FM 100-25 1999, 2-5). And "physical destruction" is a specified capability within information operations (JP 3-13 1998, I-10). Furthermore, the joint publication clearly stipulates C2W as an "application of IO."

Mark Mitchell summarizes the information operations utility for Special Operations Forces with regard to the other eight Special Operations Forces doctrinal core missions across the operational continuum of conflict. He examined Special Operations Forces "as a supporting force in a strategic IO campaign. There is also utility in using IO to enhance the effectiveness of SOF" (Mitchell 1999, 104). His interpretations are reproduced here because of the Special Operations Forces similarities to the Special Forces doctrinal core missions and to extrapolate some of his data in the next chapter regarding future missions and capabilities. On the next page, tables 2 and 3 show the information operations utility of the Special Operation Forces principal missions and collateral activity.

Table 2: IO Utility of Principal SOF Missions

	Infrastructure			Psychological		
Mission / Environment	Peace	Conflict	War	Peace	Conflict	War
Direct Action	■	■	■	▤	▤	■
Special Reconnaissance	■	■	■	▤	▤	■
Foreign Internal Defense	▤	▤	▤	■	■	■
Unconventional Warfare		▤	■		▤	■
Combating Terrorism				■	■	▤
Counterproliferation of WMD				■	■	▤
Psychological Operations				■	■	■
Civil Affairs				■	▤	▤

LEGEND

ROBUST UTILITY	MODERATE UTILITY	LIMITED UTILITY
■	▤	

(Source: Mitchell, 1999, 105)

Table 3: IO Utility of SOF Collateral Activities

	Infrastructure			Psychological		
Mission / Environment	Peace	Conflict	War	Peace	Conflict	War
Coalition Support				▤	■	■
Combat Search and Rescue					■	■
Counter Drug Activities				■	▤	
Humanitarian Demining				■	▤	
Humanitarian Assistance				■	▤	
Peace Operations				■	▤	
Security Assistance				■	▤	

LEGEND

ROBUST UTILITY		MODERATE UTILITY		LIMITED UTILITY
■		▤		

(Source: Mitchell 1999, 105)

From the draft doctrine for Army Special Operations Forces table 4 shows mutual support within the elements of C2W.

Table 4. Mutual support within the elements of C2W Mutual support within the elements of C2W

Type Unit	OPSEC	Military Deception	PSYOP	Physical Destruction	EW
Special Forces	Prevent or degrade adversary reconnaissance and surveillance against protected units and activities	Conducting physical attacks as deceptive executions Degrading adversary capabilities to see, report, and process competing observables Isolating decision maker from information at critical times to enhance effect of deception execution	Degrading adversary capabilities to see, report, and process conflicting information Degrading adversary capability to jam PSYOP broadcasts Isolating target audience from conflicting information		Reducing friendly EA target set for C2 attack by selective and coordinated destruction of adversary C2 Infrastructure targets Destroying selected electronic systems to force adversary use of systems susceptible to friendly EA/ES
SOTA	Degrade adversary reconnaissance and surveillance in EMS against protected units and activities	Conducting EA/ES as deceptive executions degrading adversary capabilities to see, report, and process competing observables Isolating decision maker from information at critical times to enhance effect of deception execution	Degrading adversary capabilities to see, report, and process conflicting information Isolating target audience from conflicting information	Providing C2 attack target acquisition through ES Destroying or upsetting susceptible assets using EMS with EA	

(Source: FM 100-25 1999, 2-14.)

Today Special Forces Operational Detachment Alpha's (ODA's) have deployable computers, digital video recorders, and Satellite communications that can transmit real-time information back to a waiting commander; whether it is the ODA's company commander at an advanced operating base (AOB) or the commander in chief in the White House situation room (Schoomaker 1998, 5). Such technology is in use today by Special Forces ODAs throughout the globe.

Modern Special Forces was born from World War II guerilla warfare. It grew and evolved learning lessons on counterinsurgency operations in during foreign internal defense missions in the sixties, seventies and eighties. Special Forces today remain centered on small unit tactics. Those tactics are core to what makes Special Forces *special* and are the unique attributes suited for warfare in the twenty-first century. The carefully selected and specially trained Special Forces soldiers that are capable of extended operations in extremely remote and hostile territory are ideally suited to be tomorrow's "warrior-diplomat." As previously exampled the flexible and adaptable Special Forces are prepared today for what future missions might arise in the information age.

In the next chapter this thesis will look forward to determine what some of those future missions will be and if they are indeed information operations missions.

CHAPTER 4

ANALYSIS

> The practical value of history is to throw the film of the past through the material projector of the present onto the screen of the future.
>
> B.H. Liddell Hart, *Thoughts on War*

In this chapter this thesis will view Hart's film; analyze those past missions, capabilities, equipment, and doctrine; and project possible missions and roles onto the screen of the future. It will also draw from the interpretations of futurist, such as Alvin and Heidi Toffler, George and Meredith Friedman, Jim Van Buskirk Jr. and Sal Raineri. In doing so it will follow the outline of the previous chapters. First, it will examine probable missions of IO. Then it will postulate possible missions that might be seen by future Special Forces soldiers. Finally, it will look at those specific missions that may be considered Special Forces information operations missions. These Special Forces information operations missions will be analyzed and set the stage for the final chapter where conclusions and recommendations will be offered for current and future Special Forces missions.

Future Information Operations

Some might say the future of IO is now. Just review the daily print of a major newspaper, visit their website or read on-line the up-to-the-minute headlines and today's true information age savvy person will see articles highlighting the latest "cyber attack" or some high technology theft. Listening to the current presidential candidates as they publicly and privately pander to the people in an effort to get their message out, one could conclude they are conducting information operations with the intensity of an all-out war. Other information operations efforts today include the Russians' campaign to paint their military offensive in Chychneya as a just cause in the world of public opinion. All of these scenarios attempt to shape the way people think and act. The strategies are diverse and different yet they all have the same ultimate goal to attain a favorable outcome for those people conducting the information operations. Just as many strategies, doctrinal principles, techniques, tactics, and procedures used in past warfare are valid and in use today, so will some past and present information operations tactics, techniques, and procedures be used in the future.

In fact, much of the future of information operations will be rooted in its past and will use those tried and true methods for achieving success. Not all information operations will be the stuff of science-fiction writers, although those aspects will play a role. The root of information operations in the future will remain unchanged. It will be as it is today-- the collection and control of information.

It could be argued that everything done in warfare is information operations. Using the Clausewitz's definition of warfare; "War is thus the act of force to compel our enemy to do our will " (Clausewitz 1993, 83). Because the intent of warfare is to change an adversary's perception that his current policies or stated intent are not advantageous, then the argument could be made that all warfare is in fact IO. However, that argument could be studied in an entire thesis on its own.

One such method for collection that will remain the same is the passing of information from one person to another. Human intelligence is as old as civilization itself and in the future will continue to be a valid method for conducting information operations. As with all missions using a specific technique, this method of IO will offer strengths and weaknesses. For example, one such strength would be to target the information operations at an individual much like the precision munitions that use one bomb to target and destroy one building. However, an inherent weakness is the slow dissemination and inevitable subtle changes as the intended information is transferred from person to person along the human chain.

When a targeted individual is the head of state, controlling the vast resources of a nation or the country's military power, then that individual will guide that entire nation's destiny through its path in history. In a more indirect approach, the targeting of a powerful advisor, wife, or significant other may influence the political leader and reap similar benefits for the opposing side. Of course an information operations campaign that is executed improperly could very well have the opposite effect from that which was intended.

The bombing of Libya by the United States in response to terrorist attacks is one example of an operation that could be argued to be an information operations campaign of the future. In that raid, code named El Dorado Canyon, the United States dropped precision munitions on Qaddafi's headquarters at the Azziziyah Barracks, the Libyan leader's nearby residence and the Bedouin-style tent he often used. They also struck the Sidi Balal terrorist training camp where there was a main complex, a secondary academy, a Palestinian training camp, and a maritime academy under construction. Qaddafi, was terribly shaken when the bombs fell near him. His house was damaged and he had reportedly injured his shoulder. For twenty-four hours, it was speculated that he had been killed. When he did reappear, he was obviously deeply disturbed and lacked his usual arrogance. Most importantly, the following months saw a decrease in the number of Libyan-sponsored, anti-American terrorist events. The Red Army Faction, one of the groups that had claimed responsibility for the La Belle disco bombing, also reduced its activities. More important, the effect of El Dorado Canyon went far beyond Libya, registering with the entire terrorist world (Boyne 1999, 3).

With the explosion of technology and the increasing use of the Internet, future information operations will continue to use mass media. The use of the mass media that began after the first printing press was built and became refined during the advent of radio and television will continue to be instrumental. In the coming century information operations will become more and more effective because of the ability to receive real-time and near real-time feedback of its effects. In its infancy today, the technology that allows for the ability to simultaneously send and receive will allow information operations to be instantly adjusted with feedback used to judge its effectiveness.

Today the Army has not yet mastered this technology and the ability to rapidly synthesize new information into an operational plan. The ability to adjust tactically has improved and it is just a matter of time and training before tomorrow's leaders at the operational level and higher will be able to seamlessly and effectively execute decisions based on the use of real time technology.

Looking into more sophisticated forms of information operations, it is inevitably to come across the science fiction writers nirvana-- the ultimate use of computers as 1s and 0s zip across interconnected networks through the atmosphere, through real space, and cyberspace. One advocate speculates, "The most potent new US weapon, however is not a bomb but a ganglion of electronic ones and zeros" (Newman 1996, 5). Computers are today and will in the future be used to conduct information operations.

In future wars, major elements of an attack will be waged in cyberspace. Former Secretary of Defense under President Ronald Regan, Casper Weinberger envisioned, "destroying and disrupting computers by using logic bombs and viruses to disrupt and disorient the enemy before the actual military assault begins" (Weinberger and Schweizer 1996, 318). In one such scenario in his book *The Next War*, Mr. Weinberger hypothesis this scenario:

> Owanda had been working on a series of complex computer programs for more than eight months. Shortly after midnight on August 20, with the massive fleet almost in place, Owada and his team inserted a series of programs into the telephone switching stations of Taiwans national telephone company. These highly potent, contagious computer viruses instantly ate the software programs that managed the country's fiber optic and telecommunications networks. Within minutes telephones and computer networks were thrown into utter chaos. Phone lines went dead, and computers locked into random programs that went nowhere. Owada then detonated eleven logic bombs which were at once fried the electronic routers directing the national railway system, air traffic control network, and maritime traffic navigational systems. (Weinberger 1996, 320)

At the operational level and tactical levels of war, Lieutenant Colonel Robert Leonhard describes situation awareness as a term in "which the commander knows the answer to three central questions: Where am I? Where are my buddies? Where is the enemy?" (Leonhard 1998, 42). An IO aid that helps the commander answer these questions is the unmanned aerial vehicle (UAV). Today UAVs are small airplane like devices that fly about the battlefield with an array of sensors or cameras to collect data and information for the commander. In the future, these devices will shrink in size and ease of operability, while simultaneously increasing in sophistication and data transmissions. With advances in technology, it is feasible that microchip dust particles can be delivered over the battlefield that would transmit continuous data for interpretation by the intelligence experts. The range of the data is limitless.

In a example of a more radical use of information operations, Dr. Vladimir Lepsky, a professor at the Institute of Psychology, Russian Academy of Science, suggests a concept he calls "reflexive control" could be used to target decision makers. Reflexive control is "related to influencing the decisions of others." Timothy Thomas writes,

> Reflexive control involves creating a pattern or providing partial information which causes an enemy to react in a predetermined fashion without the enemy realizing that he is being manipulated. Its aim, according to one Russian army officer, is to force an enemy commander to make a decision that, through the manipulation of information, was predetermined by the opposing side; or to compel the enemy to act according to a plan favorable to us. (Thomas 1999, L6-App C-3).

One aspect of reflexive control could be similar to subliminal messaging whereby a man's brain is exposed to stimuli on a subconscious level and the subject reacts reflexively yet unknowing that he has been "programmed." These imperceptible signals could be transmitted in a variety of ways, such as through radio or television, but may also include beamed laser lights, directed sound pulses, or other energy weapons.

Information operations in the future will include an integration of new technologies but will also include some old concepts. This marriage of old and new will bridge the gaps in capabilities of the different methods and enhance the total overall information operations abilities in the future.

Future Special Forces Operations

Like information operations, Special Forces operations will draw on the experiences of the past. Special Forces will continue to rely on small units of highly trained and experienced men to successfully perform difficult tasks that general purpose or conventional forces are unable to.

The core missions will remain viable Special Forces missions of the future. Special reconnaissance, direct action, unconventional warfare, foreign internal defense, and combating terrorism are all missions Special Forces will be performing in the future as they do today. How Special Forces will accomplish those future missions may change as advances in technology are integrated into both the Army and Special Forces.

Already carrying portable computers since DESERT STORM, tomorrow's Special Forces soldiers have the advantage of an acquisition section within the Special Operations Command to rapidly field new technologies. The Special Operations Acquisition and Logistics Center (SOAL) is the "USSOCOM interface with National Labs, Components, Services, Joint Staff, DoD, Congress, and Industry on Research, Development, & Acquisition Matters" (Carey Briefing 1999).

Some of these technologies will allow Special Forces soldiers to plug "acoustical hearing devices" into their ears that would amplify sounds while on clandestine reconnaissance missions (Waller 1994, 423). These devices would enhance a special reconnaissance operator's ability to gather information and in turn more information would be gathered during that mission. Microcomputers could even be built that would enable the SR team to detect the different acoustic signatures of different types of vehicles much like SONAR is able to discern different classes and types of submarines. By placing out sensors over a large area, a very small unit could collect information over a much larger area than by present conventional means. Of course with interconnectivity those sensors could also transmit directly back to the operational headquarters.

Just as the advancements in weaponry and the introduction of the machinegun changed tactical warfare, these new technologies are changing today's tactical warfare. Use of off the shelf technology communication equipment and commercial encryption capabilities have enabled adversaries to use new techniques in prosecuting their agendas. SOF equipment developers are constantly looking at new ways to counteract those abilities and maintain dominance in that arena.

In a very forward-thinking mode some are looking toward the mind itself as the weapons system. In 1994, then LTC Jim Van Bushkirk working with the Special Warfare Center put forth some of these forward concepts while being interviewed by Douglas C. Waller for his book *The Commandos: The Inside Story of America's Secret Soldiers.* Van Buskirk theorizes that there is a "better way of putting information into the computer between our ears" and suggests "hormone balances be altered with 'injectible learning' shots" (Waller 1994, 428). This would be so the brain can absorb more information. He goes on to postulate:

> Sensory enhancement devices might be implanted under the skin so the operator can see, smell, and hear objects far off. Radios might be replaced with 'synthetic telepathy'- pulse generators attached to brains so commandos can read minds instead of talking to one another on missions. (Waller 1994, 429)

The following excerpt from Waller's book is a glimpse of a possible future mission Special Forces could perform:

> The commando crawled up to the nuclear research facility that the CIA believes is secretly producing an atomic bomb. His mission has been subliminally fed into his brain by tape recorders while he slept during the plane ride to the Third World country. Sensory enhancement pills enable him to see every detail of the facility in the dark and to hear the conversations of the scientist inside. From a wristwatch radio connected to a throat mike he can communicate with the Pentagon in Washington. To divert a sentry, the commando projects a three-dimensional hologram of himself at the main gate's guardhouse. A laser beam delivers a voice projection so the hologram speaks. The commando aims his shoulder fired 'Brilliant Pebbles' rocket launcher at the facility and fires. Another neat clean operation in the twenty-first century. (Waller 1994, 419)

Is this a far-fetched scenario? Perhaps it is, but then again perhaps it is not. Wrist radios first envisioned in the 1930s Dick Tracey comics are indeed a reality today and the ability to communicate in real time directly with the Pentagon or the White House is also a reality. The roots of the information operations tree is the ability to give the right information to the right decision maker at precisely the right time so the right action is taken to ensure the sweet fruit of victory is the result.

This next section looks at the crossroads of where information operations and Special Forces missions intersect. What future Special Forces operations will be considered information operations?

Special Forces and Information Operations

In discussing both future Special Forces and information operations missions, this thesis has stated that those future missions will be rooted in the past. One core Special Forces mission that will inevitably be a part of the information operations arena is special reconnaissance. Special reconnaissance as previously discussed is "reconnaissance and surveillance actions conducted by special operations forces to obtain or verify, by visual observation or other collection methods, information concerning the capabilities, intentions, and activities of an actual or potential enemy. It includes target acquisition, area assessment, and post-strike reconnaissance" (JP 3-05 1998, GL-10).

Enhanced by available technology of direct, real-time digital video feed across broadband communications this mission is tailor made for Special Forces today and tomorrow. This will allow an infiltrated Special Forces team to send pictures directly to the headquarters command center for display to the intelligence chief, operations officers, and commander for immediate decision and action. The mission could be at a critical road or railway network junction and allow the commander the flexibility to direct his forces whether they are tanks or planes to a specific place on the ground. The target could be a specific compound or storage facility. The special reconnaissance mission could consist of making a video of bombing runs by an F-117 or B-2. After the run a battle damage assessment could be made back at headquarters and the determination made whether to reattack, or not, could be made immediately. This would prevent the delay for reattacks inherent in 24 to 36 hour air-tasking order (ATO) cycle. Live video verifying war crimes or atrocities could trigger a commander's decision to use immediate retaliatory measures and aid in the psychological campaign designed to influence the population and world opinion.

However there are drawbacks to the immediate availability of information that has not been processed or edited. There is a point at which too much information overloads a commander. Information overload can have an adverse affect on the commander's decision and even cause him to make a wrong decision. One answer to this is the integration of automation to filter or edit the data so the commander is only presented with that which is critical to his decision. This process is well rehearsed and used in the army through the military decision making process (MDMP).

Special Forces also have unique capabilities to infiltrate into politically sensitive or denied areas. The capability to access these sites could enable Special Forces teams to attack an enemy's information operations systems. In another scenario and once again drawing from one of Special Forces's core missions, direct action. A Special Forces team could move to an adversaries' hardened or underground site that was conducting information operations such as CNA or broadcasting PSYOPS thru the internet or via satellite communications (SATCOM). Once the site is positively identified they could destroy or disable it through a variety of methods. One old fashioned method of course is to use composition-4 (C4) and blow it sky high or at least the critical components. A more sophisticated approach may be to capture one of the key technicians or operators of the facility thereby de facto causing the operations to shutdown because the system could not operate without that person.

In still another scenario, specially trained technicians could be infiltrated with the Special Forces team. This technician then could directly access and input commands into a closed or secure network after the team has secured an area and gained access to a terminal linked to the network. Similarly one or more ODA members could be trained on specific commands or procedures to be executed once the terminal or an input device is accessed. Both these scenarios presume the system to be attacked is not linked to an outside network and could not be accessed remotely. Of course it may not be destruction or access that is desired but monitoring. With new technologies Special Forces teams could move in close but without direct access and monitor electronic emissions for study and analysis.

While this thesis has only looked at additional training for Special Forces soldiers on teams as they are currently configured, another method would be to completely reorganize the Special Forces team from its current force structure and skill set. This subject is too broad to be covered in this thesis but could be the basis for another study to explore that possibility.

In a final use of future Special Forces in information operations, Special Forces A-teams and B-teams conducting unconventional warfare or foreign internal defense can report feedback on the forces with whom they are working. In both cases the team's assessment on the foreign forces capabilities is passed to the JTF commander's headquarters enabling him to decide if his plan should include those forces during the operation. Furthermore with the team's direct access to the host-nation forces, host-nation civilian population and guerrilla fighters, other ongoing information operations missions such as public affairs and psychological operations can be assessed and altered as need be to fine tune a specific message at a specific targeted audience.

Looking at the future of information operations and Special Forces operations the trend is to rely heavily on electronics. In modern warfare if the electronics is taken out of information operations then "warfare reverts to the days of runners, signal flags and scraps of paper" (Adams 1998, 111). And as Adams points out on the tactical battlefield, "anything that extends the OODA (Orient, Observe, Decide, Act) loop spells danger" (Adams 1998, 111).

While Special Forces can contribute to information operations, many tasks and missions are indeed the same core missions Special Forces has successfully performed in the past and will continue to do in the future. Much of the new information operations technology will allow Special Forces to be a viable part of the JTF commander's information operations campaign. The next and final chapter will present the thesis conclusions and recommendations for the future of Special Forces in information operations.

CHAPTER 5

CONCLUSION and RECOMMENDATIONS

Purpose

This final chapter will present the conclusions drawn based on the research and presentations in the previous chapters. It will also answer the original research question posed in chapter 1: Should Special Forces doctrine expand its core missions? Finally, it will make recommendations regarding Special Forces, information operations and their integration.

This thesis has shown that Special Forces perform many tasks and missions and that these missions are an important and enhancing part of information operations; however, they are not in and of themselves information operations. In fact one officer on the Joint Chiefs of Staff in the Information Strategy Division Lieutenant Colonel Jack N. Summe has gone as far to say that information operations is not even a mission but that, "IO is an integrating strategy." In this statement I believe Lieutenant Colonel Summe has encapsulated the very heart of what information operations is and what it is not. Information operations are the integration of a vast number of missions and tasks in order to create the synergistic effect desired by the commander.

Information operations as understood by today's doctrine is not a valid core Special Forces mission. Saying that though does not discount the vital role Special Forces play in information operations now and will play in the future. This thesis has demonstrated Special Forces by their very nature have contributed immensely to the operational commander's ability to gather information and enable him to make critical decisions vital to the success of his operations. In fact, it has also shown Special Forces missions of strategic importance.

As previously stated Special Forces does indeed have a vital role in information operations. Special Forces' core missions are in fact the very missions that a CINC or JTF commander can and will integrate in his synchronization of his overall information operations plan.

For the Special Forces soldier serving in a Special Forces Group the previous five core missions are sufficiently and simultaneously broad enough and focused on what types of tasks the soldier will be performing. The technology may change some of the tactics used by Special Forces soldiers. However, adding a miniature video camera to a special reconnaissance team to provide real-time feedback to the commander does not justify calling that mission an information operations mission within the context of Special Forces doctrine. It may indeed be *part* of an overall information operation that the JTF Commander, or CINC may be conducting, but for the Special Forces soldier operating on the ground it is a de facto special reconnaissance mission with a video camera. Now, as with any new piece of equipment, the soldiers must be properly instructed and trained on its use, capabilities, and limitations in order to effectively employ and maximize its full potential.

Special Forces Groups should have the capability to conduct specific specialized missions within the information operations arena. This will require new skill sets to be acquired by Special Forces soldiers to contribute to the JTF commander's overall information operations. These skill sets should include an understanding of electronics in today's technology. This is because of today's reliance on technology. These additional skill sets should be concentrated on the use, method, and systems integration of video and audio electronic capture devices into a central processor and then the transmission of that data.

Another skill set that should be expanded on a few select Special Forces teams is the ability to use software to "hack" or "crack" into a computers security system. Because of the specialized training and time required, this skill set should be acquired just as Special Forces do with some of the other advanced specialized training. This skill set training should be given to selected individuals showing an aptitude for the skill.

These individuals would then be placed on specially identified teams within the Special Forces Group. Similar to the current specialty infiltration teams, eventually these soldiers will migrate throughout the force and their skills will become available to Special Forces teams not specifically tasked to perform that type mission. This will provide the cross-fertilization of these types of skills and enhance the initial entry-level training base on a Special Forces teams. The capability will enhance the Special Forces Group's ability to contribute to the JTF commander's information operations plan.

Possibly the most important area of information operations that Special Forces will contribute is on the staff. Since the critical link in information operations is the integration and synchronization of subordinate unit's missions, the staff is the lens through which that integration and synchronization gets focused. The new IO section envisioned in the new FM 100-6, *Information Operations* that already includes a psychological operations officer, should include a Special Forces officer. This officer may come from the SOCCE or SOCCORD and provide input to the information operations coordinator.

In the previous pages these specific recommendations have been addressed:

1. Information operations NOT be included as a new core tactical Special Forces mission. It should be added as a collateral activity and written in doctrine that Special Forces contribute to the JTF commander's IO plan.

2. Special Forces Groups should have a capability to conduct missions to penetrate a computer-based security system and retrieve data from that system.

3. The new information operations staff at the Corps and above level should include a Special Forces officer.

4. Recommend further study be done on what new skill sets might be required to enhance Special Forces' ability to contribute to the JTF commander's information operations

plan. Recommend that the study look at the training, resources, and cost associated with any new skill sets identified.

5. Recommend a study on the use of the current Special Forces organization or changes that might be needed in contributing to the JTF commander's information operations plan.

SUMMARY

Special Forces contributions to the JTF commander or CINC in accomplishing his information operations strategy and goals have been and will be significant. The unique skills that Special Forces bring to the fight are time-tested and have been shown to enhance a CINC's war-fighting ability across the operational continuum. By integrating current technology into the current skill sets and adding new skills, Special Forces will increase that enhancement and continue to remain relevant in today's changing information-based environment. Because of Special Forces' flexible abilities and mature fighting force, it will be the force of choice to accomplish the varied complex tasks that are required to deter, fight, and win against the United States' adversaries as we move forward to the twenty-first century.

GLOSSARY

Command and control warfare. (C2W) The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions.

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

Defense information infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DOD local, national, and worldwide information needs.

Defensive 10. Integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems.

Global Information Infrastructure (GII). The worldwide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users.

Information. Facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representation. The same information may convey different messages to different recipients and thereby provide "mixed signals" to information gatherers and users, to include the intelligence community.

Information Assurance. 10 that protect and defend information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

Information Environment (IE). The aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself.

Information operations (10).

Joint Pub 3-05, Joint Doctrine for Information Operations--Actions taken to affect adversary information and information systems while defending one's own information and information systems.

FM 100-6, Information Operations. 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 advantage across the full range of military operations.

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

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

National Information Infrastructure(NII). The nation-wide interconnection of communications networks, computers, databases, and consumer electronics that make vast amounts of information available to users.

Offensive 10. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers and achieve or promote specific objectives.

Special Information Operations (SIO). Information operations that, by their sensitive nature and due to their potential effect or impact, security requirements, or risk to the national security of the US, require a special review and approval process.

Special Forces (SF). US Army forces organized, trained, and equipped specifically to conduct special operations.

Special Operations Forces (SOF). Active and reserve component forces in the military services designated by the Secretary of Defense and specially organized, trained, and equipped to conduct and support special operations.

Special Operations (SO). Operations conducted by Specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or informational objectives by unconventional military means in hostile, denied, or politically sensitive areas across the full range of military operations.

REFERENCES

Adams, James, 1998. *The Next War*, New York: Simon and Shuster, 1998.

(b)(3) (10 U.S.C. 130b), (b)(6) (b)(3) (10 U.S.C. 130b), (b)(6) (b)(3) (10 U.S.C. 130b), (b)(6) interviewed by author, Fort Leavenworth, KS, March.

Barnett, Frank R., Hugh B. Tovar, and Richard H. Shultz. 1984 *Special Operations in US Strategy*, Washington, D.C.: National Defense University Press.

Boyne, Walter J. 1999 "El Dorado Canyon", *Air Force Magazine*, March, 82, No. 3.

Brodie, Bernard, and Fawn M. Brodie. 1973. *From Crossbow to H-Bomb: The Evolution of the weapons and tactics of warfare*, Bloomington: Indiana University Press.

Brown, Anthony Cane. 1982. *Wild Bill Donovan: The Last Hero*, New York: Times.

(b) (6) [redacted], S. 1998 *Urban Operations, Untrained on Terrain*, Fort Leavenworth, KS.

Campbell, Matthew, "Russian Hackers Steal US Weapons Secrets," *London Sunday Times,* July 25, 1999.

(b) (6). 1999. SOAL Overview Briefing, Joint Special Operations Intermediate Seminar. Hurlbert Field, FL, May.

Clausewtiz, Carl von. 1993. *On War*, Princeton University Press, New York.

Corbett, Julian S. *1992. Some Principles of Maritime Strategy (Classics of Sea Power Series)*, Montery, CA: Naval Institute Press.

Foch, Marshal Ferdinand. 1918. *The Principles of War*, London: H. K. Fly Co.

Furse, George Armand. 1895. *Information In War: Its Acquisition and Transmission,* London: William Clowes and Sons, Limited.

Jessup Jr., John E., and Robert W. Coakley. 1988. *A Guide to the Study and Use of Military History,* Washington, D.C., Center for Military History.

Jones, Gary M. and Christopher Tone. 1999. "Unconventional Warfare: Core Purpose of Special Forces", *Special Warfare Magazine.* 12, No. 3, 4.

Leonhard, Robert R. 1998. *The Principles of War for the Information Age,* Novato, CA: Presido Press.

Liddell-Hart, B.H. 1946. *Why Don't We Learn From History,* London: George Allen and Unwin.

Macgregor, Douglas A. 1997. *Breaking the Phalanx: A new Design for Landpower in the 21st Century,* Connecticut: Praeger.

Mitchell, Mark E. 1999. Strategic Leverage: Information Operations and Special Operations Forces, Monterey, CA: Naval Postgraduate School.

Neustadt, Richard E., and Ernest R. May. 1986. *Thinking in Time: The Uses of History For Decision Makers,* New York: The Rue Press.

Newman, Richard J. 1996. "Warfare 2020," *US News and World Report* 121. no 5.

Paddock, Dr. Alfred. 1999. "Robert Alexis McClure: Forgotten Father of Army Special Warfare," *Special Warfare* 12, No 4, 2.

Schoomaker, Peter J. 1998 Special Operations Forces: The Way Ahead, USSOCOM 5.

Stoll, Cliff, 1990. *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage* New York: Simon and Schuster.

Toffler, Alvin and Heidi. 1993. *War and Anti-War,* New York: Warner.

Thomas, Timothy L. 1996. "Russian Views On Information-Based Warfare", *Air Power Journal,* Special Edition.

Thomas, Timothy L. 1999. "The Russian PSYOP and Information Operations Interface," *Information Operations, USACGSC, A544 Lesson 6.*

Tzu, Sun, 1963. *The Art of War,* Translated by Samuel B. Griffith, London, Oxford Press.

U.S. Code, Title 10, section 167

U.S. Department Air Force. 1997. AFDD-1, *Air Force Basic Doctrine.* September.

U.S. Department of the Army. 1998. FM 31-20, Doctrine for Army Special Forces Operations (Draft). December.

U.S. Department of the Army. 1969. FM 31-21, *Special Forces Operations*. February.

U.S. Department of the Army. 1999. FM 100-6, *Information Operations: Tactics, Techniques, and Procedures, Initial Draft.* 30 April.

U.S. Department of the Army. 1998. FM 100-25, *Doctrine for Army Special Operations Forces (Final Draft)*. 30 April.

U.S. Department of Defense. 1998. Joint Pub 3-05*, Joint Doctrine for Special Operations.* 17 April.

U.S. Department of Defense. 1998. Joint Pub 3-13, *Joint Doctrine for Information Operations*, 9 October.

U.S. Department of Defense. 1975. DoD GEN-36, *The Armed Forces Officer*, Washington D.C.: American Forces Information Service.

U.S. Department of Defense. 1998. USSOCOM Pub 1, United States Special Operations in Peace and War.

U.S. Department of Defense, 1998. USSOCOM Special Operations Reference Manual. January.

U.S. Department of Defense. 1999. Briefing: The Son Tay Prisoner of War Rescue Operation, Joint Special

Operations Intermediate Seminar. Hurlburt Field, FL, May.

U.S. Special Operations Command Briefing. 1999. Joint Special Operations Intermediate Seminar, Hurlburt Field, FL, May.

Waller, David C., 1994. *The Commandos: The Inside Story of America's Secret Soldiers*, New York: Dell Publishing.

Watson, Bruce W. Bruce George, Peter Tsouras, and B.L. Cry. 1993. *Military Lessons of the Gulf War*, California: Presidio Press.

Weinberger, Casper, and Peter Schweizer. 1996. *The Next War*, Washington, D.C.: Regnery Publishing Inc.

INITIAL DISTRIBUTION LIST

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

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

3. SOTD Joint Readiness Training Center
Fort Polk, LA 71459

4. (b) (6) [redacted]
HHC, Garrison Command
Fort Leavenworth, KS 66027

5. (b) (6) [redacted] [redacted]
410 Kearny
Fort Leavenworth, KS 66028

6. (b) (6)
CTAC
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

7. (b) (6) [redacted]
3021 Lucille
Ashland, KY 41102-5253

8. (b)(3) (10 U.S.C. 130b), (b)(6) (b)(3) (10 U.S.C. 130b)
HHC, 3rd Special Forces Group (Airborne)
Fort Bragg, N.C. 28310

9. (b)(3) (10 U.S.C. 130b), (b)(6). (b)(3) (10 U.S.C. 130b)
HQ, 7th Special Forces Group (Airborne)
Fort Bragg, N.C. 28310

10. (b)(3) (10 U.S.C. 130b), (b)(6)
HHC, 5th Special Forces Group (Airborne)
Fort Campbell, KY 42223

11. (b) (6)
USASAMS
USACGSC
1 Reynolds Ave.
Fort Leavenworth, KS 66027-1352

12. (b)(3) (10 U.S.C. 130b), (b)(6)
HQ, 5th Special Forces Group (Airborne)
Fort Campbell, KY 42223-6214

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 2 June 2000

2. Thesis Author: (b) (6)

3. Thesis Title: Information Operations: A valid Special Forces Core Mission?

4. Thesis Committee Members

   Signatures: (b) (6)

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

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

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

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

EXAMPLE

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

Fill in limitation justification for your thesis below:

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

________________ / __________ / __________

________________ / __________ / __________

________________ / __________ / __________

________________ / __________ / __________

________________ / __________ / __________

7. MMAS Thesis Author's Signature: ________________________

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

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

1. Foreign Government Information. Protection of foreign information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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