

NAVAL POSTGRADUATE SCHOOL

Monterey, California



THESIS

STRATEGIC LEVERAGE: INFORMATION OPERATIONS AND SPECIAL OPERATIONS FORCES

by

Mark E. Mitchell

March 1999

Thesis Advisor:

John Arquilla

Approved for public release; distribution is unlimited.

19990218188

REPORT DOCUMENTATION PAGE

Form Approved OMB No.
0704-0188

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

1. AGENCY USE ONLY (Leave blank)

2. REPORT DATE

March 1999

3. REPORT TYPE AND DATES COVERED

Master's Thesis

4. TITLE AND SUBTITLE: Strategic Leverage: Information Operations and Special Operations Forces

5. FUNDING NUMBERS

6. AUTHOR(S)

Mark E. Mitchell

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

Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING
ORGANIZATION REPORT
NUMBER

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

10. SPONSORING /
MONITORING AGENCY
REPORT NUMBER

11. SUPPLEMENTARY NOTES

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Special Operations Forces (SOF) have assumed a unique and expanded role as a strategic asset of the United States. The conjunction of changing political and security environments and new technologies present both challenges and opportunities for SOF. Special Operations Forces provide the National Command Authority (NCA) a variety of unique capabilities and expanded options for achieving strategic goals at minimum costs. The recent drawdown has placed even more value on the capabilities and leverage provided by SOF. Additionally the rapid pace of technological change – the “information revolution” – has opened the door to a potential “Revolution in Military Affairs” (RMA). New approaches to warfare, like Information Operations (IO), are beginning to emerge from the RMA.

Information operations, like SOF, can also provide a means to leverage limited resources. At the strategic level, SOF can provide support for IO; at the tactical level, IO can support of special operations (SO). Each has distinct implications for SOF. In either case, the object of the supporting operation is to generate or expand a window of opportunity for the supported operation. Separately, both SO and IO can provide economy of force. Properly employed, this leverage is multiplied and offers a tremendous strategic asset.

14. SUBJECT TERMS

Information Operations, Information Warfare, Special Operations, Special Operations Forces (SOF)

15. NUMBER OF
PAGES

244

16. PRICE
CODE

17. SECURITY CLASSIFICATION OF
REPORT

Unclassified

18. SECURITY CLASSIFICATION
OF THIS PAGE

Unclassified

19. SECURITY CLASSIFI- CATION OF
ABSTRACT

Unclassified

20. LIMITATION
OF ABSTRACT
UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. Z39-18

Approved for public release; distribution is unlimited

**STRATEGIC LEVERAGE: INFORMATION OPERATIONS AND SPECIAL
OPERATIONS FORCES**

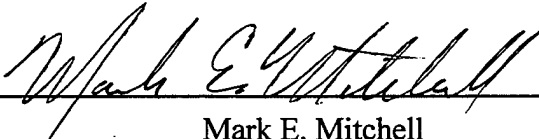
Mark E. Mitchell
Major, United States Army
B.S., Marquette University, 1987

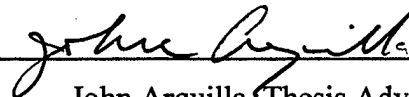
Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

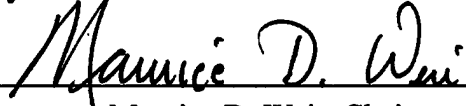
from the

**NAVAL POSTGRADUATE SCHOOL
March 1999**

Author: 
Mark E. Mitchell

Approved by: 
John Arquilla, Thesis Advisor


Gordon McCormick, Second Reader


Maurice D. Weir, Chairman
Special Operations Curriculum Committee

ABSTRACT

Special Operations Forces (SOF) have assumed a unique and expanded role as a strategic asset of the United States. The conjunction of changing political and security environments and new technologies present both challenges and opportunities for SOF. Special Operations Forces provide the National Command Authority (NCA) a variety of unique capabilities and expanded options for achieving strategic goals at minimum costs. The recent drawdown has placed even more value on the capabilities and leverage provided by SOF. Additionally the rapid pace of technological change – the “information revolution” – has opened the door to a potential “Revolution in Military Affairs” (RMA). New approaches to warfare, like Information Operations (IO), are beginning to emerge from the RMA.

Information operations, like SOF, can also provide a means to leverage limited resources. At the strategic level, SOF can provide support for IO; at the tactical level, IO can support of special operations (SO). Each has distinct implications for SOF. In either case, the object of the supporting operation is to generate or expand a window of opportunity for the supported operation. Separately, both SO and IO can provide economy of force. Properly employed, this leverage is multiplied and offers a tremendous strategic asset.

TABLE OF CONTENTS

I. INTRODUCTION	1
A. PURPOSE	1
B. BACKGROUND	1
1. The New Security Environment	5
2. A Continued Demand for SOF	12
3. The Revolution in Military Affairs	13
C. RESEARCH QUESTIONS	18
D. FINDINGS	18
E. METHODOLOGY	18
F. ORGANIZATION	19
II. INFORMATION OPERATIONS	21
A. INFORMATION WARFARE VS. INFORMATION OPERATIONS	24
B. INFORMATION-IN-WAR AND INFORMATION OPERATIONS	26
C. CONCEPTS OF INFORMATION OPERATIONS	37
1. Information Systems Approach	40
2. The Psychological Approach	53
3. Other Views	63
4. Defensive Information Operations	69
D. SUMMARY	71
III. THE STRATEGIC INTEGRATION OF SOF AND IO	73
A. SOF CORE COMPETENCIES	74
1. Access	75
2. Regional Orientation	79
3. Adaptability	81
B. THE STRATEGIC UTILITY OF SPECIAL OPERATIONS	82
1. Economy of Force	84
2. Expansion of Choice	85
3. Tailor-to-Task Capabilities	87

4. Other Uses	87
5. The Misuse of SOF.....	90
C. INTEGRATING SOF AND IO	93
1. Supporting the Psychological Approach	93
2. Supporting the Infrastructure Approach.....	98
3. Supporting Defensive IO	99
D. ADVANTAGES OF INTEGRATION	102
E. SUMMARY	103
IV. THE TACTICAL INTEGRATION OF SOF AND IO	107
A. THE DECISION CYCLE (THE OODA LOOP)	107
B. THE CONCEPT OF RELATIVE SUPERIORITY.....	110
C. USING IO TO ACHIEVE AND SUSTAIN RELATIVE SUPERIORITY	115
1. Observe.....	116
2. Orient.....	119
3. Decide.....	123
4. Act	125
D. IO SUPPORT FOR EXTENDED-DURATION SPECIAL OPERATIONS	126
1. Sequential and Cumulative Strategies	127
2. Support for Unconventional Warfare	129
3. Support for Other SOF Missions and Collateral Activities.....	130
E. POST MISSION IO SUPPORT	131
F. THE ADVANTAGES OF INTEGRATION	132
G. SUMMARY	132
V. THE FUTURE OF SOF ROLES AND MISSIONS	135
A. THE ROLES AND MISSIONS DEBATE	136
B. THE ROLES AND MISSIONS OF SOF	139
C. ACCEPTING IO AS A MISSION FOR SOF	143
1. Criteria for New Missions	144
2. Evaluating IO as a SOF Mission	146

3. Preparing SOF to Conduct IO	147
D. SUMMARY	149
VI. CONCLUSION	151
A. SUMMARY	151
B. ISSUES OF INTEGRATION	159
1. Characteristics of Integrated SOF/IO	159
2. Obstacles to integration	161
C. ISSUES OF STRATEGY	162
1. IO and Deterrence	164
2. IO Concepts and the Analogy to Sea Power	169
3. Strategic Emphasis	171
D. CONCLUSION	176
E. RECOMMENDATIONS FOR FUTURE RESEARCH	177
APPENDIX A. GLOSSARY OF DoD DEFINITIONS	179
APPENDIX B. GLOSSARY OF COMPUTER SECURITY TERMS	193
APPENDIX C. SOF MISSIONS AND COLLATERAL ACTIVITIES	203
A. PRINCIPAL MISSIONS	203
B. COLLATERAL ACTIVITIES	205
APPENDIX D. IW/IO DEFINITIONS	209
A. INFORMATION WARFARE:	209
B. INFORMATION OPERATIONS	211
C. OTHER DEFINITIONS	212
BIBLIOGRAPHY	215
INITIAL DISTRIBUTION LIST	225

LIST OF FIGURES

Figure 4-1: Boyd's OODA Loop Model of Rational Decision-Making	108
Figure 4-2: Generic Relative Superiority Graph.....	112
Figure 4-3: RS Achieved before Mission Execution	118
Figure 4-4: Expanding Relative Superiority	121
Figure 4-5: Sustaining Relative Superiority.....	124

LIST OF TABLES

Table 1-1: Military End Strength (thousands) 1992-1999.....	8
Table 1-2: U.S. Defense Expenditures (billions \$) 1992-1999.....	10
Table 2-1: Critical Infrastructure Categories and Elements.....	42
Table 2-2: Summary of IO Concepts	71
Table 3-1: IO Utility of Principal SOF Missions.....	105
Table 3-2: IO Utility of SOF Collateral Activities.....	106
Table 5-1: Traditional and Current Roles and Missions of SOF	143
Table 6-1: IO Support for the National Military Strategy.....	163

ACKNOWLEDGEMENTS

I would like to thank my wife, Mary Ann, and daughter, Caroline, for their generous support and understanding. I would also like to thank Dr. John Arquilla, for his invaluable advice, insights, and encouragement.

I. INTRODUCTION

A. PURPOSE

The purpose of this thesis is to investigate the relationship between Special Operations Forces¹ (SOF) and Information Operations (IO) and the potential for combining them to optimize limited resources. It will explore their respective abilities to affect the course and outcome of a conflict, i.e. their strategic utility. It will examine how the special skills, innovative tactics, and organizational agility of SOF can support or complement IO at the strategic level. The potential for IO to provide support to special operations (SO) is also examined. It will also probe the consequences of the "Revolution in Military Affairs" (RMA) for SOF and the types of strategic missions which SOF should be prepared to conduct in the coming decades, i.e. roles and missions for SOF.

B. BACKGROUND

Special Operations Forces have assumed a unique and expanded role as a strategic asset of the United States. Special Operations Forces offer a collection of capabilities that is not available elsewhere in the Armed Forces of the United States. While other organizations may possess some of the same capabilities, no other organization possesses this unique assortment.

¹ For the purposes of this thesis, Special Operations Forces consist of the organizations, active and reserve, assigned to the United States Special Operations Command (USSOCOM) and its subordinate commands. This includes forward deployed forces of those subordinate commands under the control (e.g. Combatant Command (COCOM)) of the regional Commanders in Chief (CINCs).

Special operations differ from traditional military operations in degree of political risk, often unconventional mode of employment independence from friendly support, and their dependence on detailed intelligence and indigenous assets. For these reasons, some SOF missions carry an exceptionally high degree of physical risk. Because of the political sensitivities surrounding many SOF missions, where failure can damage national prestige, close coordination at the interagency level between DoD and other U.S. government agencies is necessary. Close interagency coordination maximizes SOF effectiveness in the political-military environment short of war.²

Since the establishment of the US Special Operations Command (USSOCOM) in 1987, the role of Special Operations Forces (SOF) in peace, conflict, and war, has increased steadily. These forces provide the National Command Authority (NCA) a variety of unique capabilities and expanded options for achieving strategic goals with lower levels of cost and risk.

The current National Security Strategy (NSS) is based on, among other things, the principle of political engagement. The broad range of capabilities possessed by SOF support this, as well all three pillars of the National Military Strategy (NMS) - shaping the international environment, responding to the full spectrum of crises, and preparing now for an uncertain future. Shaping the international environment requires building relationships with allies and partners that instill trust and confidence. SOF expand national capabilities to react to sensitive situations, including noncombatant missions such as humanitarian assistance, security assistance, and peace operations. The language capabilities, cultural awareness, and frequent deployments of SOF readily support this

² Department of Defense, *Annual Report to the President and the Congress*. Washington D.C.: Dept. of Defense, 1998. n.pag. Online. Internet. Available: www.dtic.mil/execsec/ad98

endeavor by establishing enduring links with the military and civilian leaders and local populations.

The skills of SOF are applicable across the operational spectrum; from large-scale operations to smaller contingencies, SOF skills enhance the ability of the United States to respond quickly and effectively to any situation. Finally, SOF is often on the cutting edge in adopting new capabilities and technologies. These abilities, when coupled with the doctrinal and organizational flexibility of SOF, offer an effective solution to preparing for uncertain threats.

SOF also present the NCA and uniformed decision-makers with expanded options by providing a flexible and capable force. They expand the range of options available to decision makers confronting crises and conflicts below the threshold of war, such as terrorism, insurgency, and sabotage. The organizational agility of SOF, coupled with rapidly adaptable skills, allow quick tailoring of force packages to tackle a wide range of tasks under varying conditions across the entire operational spectrum. These force packages are also tailored to specific missions more easily than conventional forces.

The relatively small size of SOF, in combination with unique capabilities and organizational agility, means that SOF can provide a highly leveraged force. Comprising just over two percent of the total force³, SOF "may be most effective in conducting

³ According to USSOCOM, the total SOF end-strength for 1999 is 46,134 (this includes 13,823 members of reserve and National Guard forces). Active duty end strength is 29,533 personnel, which accounts for 2.11 percent of the total active force of 1.395 million personnel. United States Special Operations Command (USSOCOM), *United States Special Operations Forces: Posture Statement 1998* (Washington, D.C: Government Printing Office), 17.

economy of force operations, generating strategic advantage disproportionate to the resources they represent.”⁴ SOF can provide economy of force by “reinforcing, augmenting, supplementing, and complementing conventional forces” across the spectrum of conflict and during all phases of a conflict.⁵

Changing political and security environments combined with new technologies present both challenges and opportunities for SOF. As General Peter J. Schoomaker, Commander in Chief of USSOCOM, recently wrote:

The revolutionary capabilities offered by Information Age technologies are forcing us away from traditional assumptions about SOF organization and even the conduct of operations.⁶

Force reductions and budgetary constraints have placed even more value on the capabilities, leverage, and value provided by SOF. Additionally, the rapid pace of technological change – the “information revolution” – has opened the door to what many are calling a “Revolution in Military Affairs” (RMA). New approaches to “warfare” like Information Operations (IO) are beginning to emerge from the RMA. Proponents believe that IO has the potential, like SOF, to provide a means of leveraging limited resources and achieving strategic objectives.

⁴ Peter J. Schoomaker, “U.S. Special Operations Forces: The Way Ahead.” *Special Warfare*, Winter 1998: 4.

⁵ USSOCOM, *Posture Statement 1998*, 5.

⁶ Schoomaker 6.

1. The New Security Environment

As we approach the 21st century, the United States faces a dynamic and uncertain security environment. We are in a period of strategic opportunity. With the end of the Cold War and the dissolution of the Warsaw Pact, the threat of global war has receded. The values that we hold dear -- freedom, democracy, and market economics -- are being embraced in many parts of the world. Meanwhile, the changing global economy and proliferation of international information systems continue to transform culture, commerce, and global interaction.⁷

Allen H. Holmes

The end of the Cold War has radically changed the international security environment. Many of the principles and assumptions that guided defense policy during the Cold war may no be longer applicable. The survival of the United States is not threatened by a competitor with comparable economic and military capabilities.⁸ It appears that it will be at least a generation before the United States faces a peer competitor. This does not mean that there is no longer any threat, only that the nature of the threat has changed. The 1997 Quadrennial Defense Review identified five primary risks facing the United States in the next 20 years:

- Regional dangers from would-be regional hegemony to instability generated by failing or failed states.
- Proliferation of sensitive information and technology -- especially nuclear, biological, and chemical weapons and their means of delivery.
- Transnational dangers, such as illegal drug trade or organized crime.
- Threats to the United States and its citizens through terrorism or information warfare.

⁷ H. Allen Holmes, "Military Operations in the Post Cold War Era," Intelligence in Partnership Conference, Joint Military Intelligence Conference, Andrews AFB Maryland, June 26, 1997. Reprinted in *Defense Issues*, Vol. 12, No. 34.

⁸ However, it must be noted that Russia still maintains nuclear parity with the United States despite the collapse of the Soviet Union.

- Adversaries likely to pursue asymmetric means that attempt to circumvent U.S. strengths and attack perceived vulnerabilities.⁹

Demographic trends, particularly increasing population and urbanization, are likely to intensify some of these threats. It is difficult to predict with any certainty which one will pose the greatest threat to national interests at any given time. Superiority on the conventional battlefield is not a guarantor of peace or security. The technological superiority of the United States may force our opponents to turn to asymmetric strategies and capabilities to counter our technological edge. For many nations, the lesson learned as a result of overwhelming superiority of US forces in the Gulf War may have been that it is futile to attempt to go toe-to-toe against the full weight of the US military might. This means that the nature of the “battlefield” may change as our adversaries and competitors (nations or other entities) are unwilling to confront us on the conventional battlefield. This dynamic is evident in the growing number of states seeking to develop “weapons of mass destruction” (WMD). In the words of H. Allen Holmes, Assistant Secretary of Defense for Special Operations/Low Intensity Conflict, “The world remains a highly uncertain place with increasingly complex and dangerous national security threats.”

Engagement is the imperative of the National Security Strategy and the National Military Strategy (NMS) – “Shape, Respond, Prepare” – demands that U.S. forces operate across the spectrum of conflict. The armed forces of the United States, with military capabilities developed during the Cold War to meet the global challenge of the Soviet Union, have struggled to adapt to this demand in an increasingly complex and dynamic

⁹ Earl H Tilford Jr., ed., *World View: The 1998 Strategic Assessment from the*

environment. Crisis intervention, disaster relief, humanitarian assistance, and peacekeeping are all examples of the increasingly diverse and non-traditional missions tackled by the United States military. The requirements of these missions coupled with those of missions that are more traditional have dramatically increased the number and frequency of deployments for all services. According to the Secretary of the Army:

The increase in the number of military operations since 1989 is one of the most striking features of the post-Cold War world. America's Total Army is a busy Army. On any given day in 1997, the Army had, on average, over 31,000 active and reserve soldiers and civilians deployed in over 70 countries, not counting the 100,000 forward-deployed soldiers. In May 1997, worldwide deployments reached the 100-country mark for the first time in the Army's history. Such involvement does not come without costs. We are doing more with fewer people, performing three times more deployments than during the Cold War.¹⁰

The pressure to complete these tasks in a timely manner with limited resources has increased. At the same time the nature of missions has changed and the number of missions multiplied, the resources available to accomplish these missions have decreased. A provision in the FY 1999 Defense Budget expresses the sense of Congress that the readiness of U.S. military forces to execute the national security strategy is being eroded by this combination of declining defense budgets and expanded missions, including the peacekeeping mission in Bosnia, and that defense appropriations are not keeping up with

Strategic Studies Institute, (Carlisle Barracks: US Army War College, 1998), 20.

¹⁰ Department of Defense, "Report of the Secretary Of The Army," *Annual Report to the President and Congress* (Washington, D.C.: Government Printing Office, 1998). Although this is just one service, the other service secretaries note similar increases in their respective reports.

military needs.¹¹ A House report on readiness stated that "The expanding demands of peacekeeping and humanitarian operations... are placing at risk the decisive edge that this nation enjoyed at the end of the Cold War..."¹²

Table 1-1: Military End Strength (thousands) 1992-1999

Fiscal Year	Active Forces	Reserve Forces	TOTAL
1992	1808.1	1114.9	2923.0
1993	1705.1	1057.7	2762.8
1994	1610.5	998.3	2608.8
1995	1518.2	945.8	2464.0
1996	1471.7	920.4	2392.1
1997	1438.6	902.2	2340.8
1998	1419.3	886.1	2305.4
1999 (est.)	1395.8	877.1	2272.9

Source: Department of Defense, *1998 Annual Defense Report*, Appendix B. Online. Internet. Available: www.dtic.mil/execsec/ad98/apdx_b.html

Despite reductions in manpower and infrastructure, the financial resources available to the Department of Defense remain restricted. In real terms, the defense budget of the United States has declined every year since 1989 except 1992. According to recent congressional testimony by the Joint Chiefs of Staff the budget strain has been exacerbated by the unexpected costs incurred as a result of performing the missions

¹¹ United States Public Law 105-262, (H.R.4103 Sec. 8160) Approved:10/17/98 Available <http://rs9.loc.gov/cgi-bin/bdquery/z?d105:HR04103:/>

¹² United States House of Representatives, Committee on National Security, *Military Readiness 1997: Rhetoric and Reality* (Washington, D.C.: Government Printing Office, 1997) 1.

mentioned above.¹³ The omnibus appropriations measure adopted in the final hours of the 1998 allocated an extra \$8 billion as "emergency spending" to alleviate some of the strain.¹⁴ While this additional money is helpful, it does not provide along term solution to the fiscal problems caused by the changing security environment. A analysis by the Center for Strategic and Budgetary Analysis warns that "unless DoD transforms itself into a very different kind of military, it will be unable to effectively meet the very different kinds of challenges likely to exist in the future."¹⁵

¹³ Bradley Graham, "Senators Scold Military Chiefs: Top Officers Accused of Failing to Warn Soon Enough of Readiness Decline." *Washington Post*, 30 September 1998.

¹⁴ George C. Wilson, "105th Review: Pentagon Gets Extra Money As Key Issues Remain Unresolved." LEGI-SLATE News Service 26 Oct 1998. Online. Internet. Available: www.legislate.com

¹⁵ The Center for Strategic & Budgetary Assessments, *Military Readiness: Good News, Bad News and Questions for the Future*. 24 September 1998. Online. Internet. Available: www.csbahome.com

Table 1-2: U.S. Defense Expenditures (billions \$) 1992-1999

Fiscal Year	Actual Defense Budget (Billions of \$)	Adjusted Defense Budget (in 1996 \$)	% Real Growth
1992	\$ 281.8	\$ 329.6	0.1
1993	\$ 267.4	\$ 303.8	(7.9)
1994	\$ 251.3	\$ 279.1	(8.1)
1995	\$ 255.6	\$ 278.4	(0.2)
1996	\$ 254.4	\$ 271.3	(2.6)
1997	\$257.9	\$269.1	(0.8)
1998	\$254.9	\$260.1	(3.4)
1999	\$257.2	\$257.2	(1.1)

Source: Department of Defense, *1998 Annual Defense Report*, Appendix B. Online. Internet.
Available: www.dtic.mil/execsec/ad98/apdx_b.html

In addition to fiscal constraints, today's forces are confronted with additional operational constraints: many of the new missions require discriminate and discrete engagement for domestic and international political reasons. In many circumstances, a low-profile American presence is not only desirable but also necessary. Additionally, performing almost any mission with minimal casualties (both military and civilian) is perceived, domestically and internationally, as an achievable goal. This does not imply that a concern for casualties has been non-existent but rather that the threshold is lower in the absence of threats to vital national interests or the survival of the United States. ¹⁶ The American public has shown a willingness to support casualties when vital national

interests are at stake but it has become more difficult to identify those *vital* interests in the Post-Cold War era.

Because of these factors, the Armed Forces of the United States are required to accomplish more tasks with fewer resources in a dynamic and uncertain environment. With the greatly reduced force and increased commitments the need to carefully apportion constricted resources and still achieve the desired results demands flexibility and leveraging whenever possible.

This is particularly true of SOF. SOF will have limited resources and it is unlikely that the size of special operations forces will change significantly over the next decade. This is not to say that there may not be pressure to expand the size of SOF because of increasing demand. Regardless of the pressures, USSOCOM is unlikely to meet the increased demand unless there is some shift in priorities or missions. There are several reasons for this. The first is the restricted resources noted above; the defense budget is likely to remain relatively stable for the next decade. An increase on the scale of the Reagan Buildup is nearly unthinkable in the absence of a peer competitor. Additionally, bureaucratic politics is likely to prevent SOF from consuming a much larger share of the existing pie, even if the budget is increased. The force modernization plans of each service are likely to receive the lion's share of any increase in the defense budget.

A second factor that will constrain the growth of SOF is the problem associated with the mass-production of SOF. Even with an increased budget, quality control will

¹⁶ Eric V. Larson, *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica: Rand, 1996) xvi.

always be an issue. SOF already has problems recruiting and training qualified candidates because the drawdown has decreased significantly the size of the recruiting pool with while SOF force structure has remained stable. U.S. SOF have consistently refused to sacrifice quality for quantity and they unlikely to lower their standards. Barring some massive (and unlikely) shift in the quality and quantity of recruits, there will not be a significant change in the number of people who successfully complete the selection, assessment, and initial training required by SOF. The bottom line is that there are a finite number of people who are both willing to make the commitment and capable of the level of performance demanded by SOF.

A third factor that will constrain the growth of SOF is the potential for deleterious effects on conventional forces. Eliot Cohen identified some potential negative effects of large elite units, including “skimming the cream,” and weakening of command and control.¹⁷ It is unlikely that conventional force commanders would stand by idly as large numbers of high quality personnel left to join expanded SOF. Further, the service chiefs would probably attempt constrain the growth of USSOCOM, which could pose a bureaucratic threat because of its service-like nature.

2. A Continued Demand for SOF

If the United States is to remain engaged in a dynamic environment with numerous non-state threats there will be some requirement for SOF. As the geo-strategic landscape has shifted, the core competencies of SOF have provided exceptional value

¹⁷ Eliot Cohen, *Commandos and Politicians: Elite Units in Modern Democracies*. (Cambridge: Harvard Center for International Affairs, 1978) 53-60.

around the globe. Indeed, SOF is already the force of choice for combating some of these threats. While some conventional forces (most notably the Marine Corps) are likely to develop some of the specialized skills found in SOF, they cannot replace SOF. Conventional forces are unlikely to acquire the language skills or political and cultural sensitivity of SOF; there are simply not enough resources to develop language skills on a broad basis. Conventional forces are also unlikely to acquire the same advanced equipment as SOF, although some diffusion is inevitable. Finally, conventional forces cannot duplicate the maturity and experience that are the hallmarks of SOF operators. In any case, it is likely that there will always be some skills or capabilities not available in the conventional force. Therefore, there will be an enduring requirement for SOF. However, SOF must confront the realities of limited resources and increasing demand. A potential, if only partial, solution to this dilemma may be found in the new capabilities offered by the budding Revolution in Military Affairs (RMA).

3. The Revolution in Military Affairs

By most accounts, we have entered the "Information Age" where information is supplanting, to some extent, the machines of the Industrial Age as the driving social and economic force. This change will present both threats and opportunities for SOF; the diffusion of information technology can and will change the environment in which SOF operate. The nature of the information revolution is different from that of the industrial revolution. It is entirely possible that non-industrialized nations will make a quantum leap forward into the information age. They may never reach the same level as the United States, Japan or Germany but they can make enormous progress in short periods. Even the

diffusion of technologies that we take for granted, e.g. cellular telephones and the Internet, can radically alter a society. Consequently, the potential for a "Revolution in Military Affairs" (RMA) has received a lot of attention recently. The essential concept is that advances in information technology will enable innovations that fundamentally alter the conduct of military operations; it is an attempt to leverage technological superiority into strategic superiority.

Historian Michael Roberts advanced the notion of an RMA based on his study of 16th Century Swedish infantry tactics. Roberts outlined four characteristics of an RMA: a radical shift in tactical doctrine; a substantial change in the size of armies; a dramatic change in strategy, and an effect on society. Andrew Marshall, former Director of the Office of Net Assessment offers this definition:

A Revolution in Military Affairs is a major change in the nature of warfare brought about by the innovative application of new technologies which, combined with dramatic changes in military doctrine and operational and organizational concepts fundamentally alters the character and conduct of military operations.¹⁸

Andrew Krepinevich offers a similar definition of an RMA:

[W]hat occurs when the application of new technologies into a significant number of military systems combines with innovative operational concepts and organizational adaptation in a way that fundamentally alters the character and conduct of conflict. It does so by producing a dramatic increase--often an order of magnitude or greater--in the combat potential and military effectiveness of armed forces.¹⁹

¹⁸ Qtd. in SAIC Strategic Assessment Center. *The Revolution in Military Affairs*, Online. Internet. Available: www.sac.saic.com

¹⁹ Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest* Fall 1994: 30.

Both of these definitions are less restrictive than Roberts' definition; they do not mention a requirement for an effect on society. Whether this is a necessary condition for a revolution in *military* affairs is debatable but they are in general agreement on the aspects of an RMA. History is replete with examples of technological innovations but the number of revolutions in military affairs is more limited. A primary reason for this is that improvements in technology alone do not constitute a revolution – doctrine, tactics, and organizational changes must occur.

From the point of view of some authors, the Gulf War marked the initial departure from the “mass-based warfare” which had been dominant since the industrial revolution, and the start of a revolution in warfare.²⁰ Others have hailed the Gulf War as the first “information war,” primarily because of the use of precision guided munitions and advanced communications.²¹ This viewpoint is unsupported by the facts, however. Regardless of the introduction of new technology on the battlefield, the degree of doctrinal, tactical, or organizational innovation was almost imperceptible. The military strategy employed in the Gulf War was derived from Clausewitz and focused on the physical destruction of the enemy. Despite the employment of some advanced

²⁰ Edward Mann, “Desert Storm: The First Information War?” *Air Power Journal* Vol. VIII, No. 4 (Winter 1994): 14. “A new chapter in warfare was written on 17 January 1991. With the advent of postindustrial warfare, information warfare, or knowledge warfare--whatever one might choose to call it--a window opened, giving discerning people an opportunity to gaze into the future. Although the view remains blurred and imperfect, warriors who make the most of it increase their chances for victory in the next round.”

²¹ Alvin Toffler, and Heidi Toffler, *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner, 1995) 76-77.

technology and some innovative organizational arrangements, the organization of the forces and the tactics were, as a whole, very traditional. The United States and the allied coalition concentrated massive ground forces in the theater of operations, employed established doctrine and tactics, and relied upon the control and penetration of enemy air space. Eliot Cohen observed that the "most of the ordnance ...consisted of 1950s-technology unguided bombs dropped by aircraft developed in the 1960s or in some cases the 1970s."²²

It is likely that the question of whether we are truly in the midst of an RMA will only be answered authoritatively in the future, from a historical perspective. Nonetheless, the increasing pace of technological advances at least holds the possibility that warfare may be revolutionized. Two things are certain though: technology is changing rapidly and technology alone offers no guarantee of success. The painful U.S. debacle in Somalia and Russian problems in Chechnya provide ample evidence of the latter.

Technology is a double-edged sword; it may prove difficult to prevent the diffusion of many of the emerging technologies to our adversaries. The net result is that other nations may have access to the same, or similar, technologies as the United States or, more importantly, to effective countermeasures to our technologies. The United States currently maintains a distinct technological advantage over the rest of the world but technological change is not limited to the United States, nor is it confined to the government sector. The majority of technological advances are occurring in the private

²² Eliot Cohen, "A Revolution in Warfare," *Foreign Affairs* March/April 1996, 39.

sector and it is becoming increasingly difficult to limit the diffusion of technology. There are no guarantees that the US can contain the spread of technology or even maintain a significant technological edge. This point is amply demonstrated by attempts to control "weapons of mass destruction" (WMD). If we cannot control the spread of deadly technologies, how much harder will it be to control the spread of non-lethal technologies?

Modern technological developments are changing the way our adversaries, and we, approach conflicts. Mindful of the limitations on technology, the United States must still endeavor to exploit any advantage that technological innovation may provide. Improved battlefield communications, better collection and dissemination of intelligence, and greater lethality of weapons are a few of the obvious applications of technology. Largely though these applications have been only evolutionary – simply enhancing existing systems, doctrine, and organizations. Since the strategy and organizations for employing them have not changed significantly, it is difficult to characterize the changes that have occurred as a true "revolution".

The concepts of Information Warfare (IW) and Information Operations (IO) represent, to a degree, new strategies for employing emerging technologies. Admittedly, they encompass some age-old concepts but it is in the conceptual, strategic, and organizational integration of these old concepts and the innovative application of emerging technology that the revolutionary potential of IO lies. For SOF, IO presents an opportunity to redress the imbalance in resources and demand by enhancing the efficiency of current forces.

C. RESEARCH QUESTIONS

This thesis will attempt to answer the following questions:

1. What constitute "Information Operations"?
2. What is the strategic utility of Information Operations?
3. How can SOF and IO be integrated to achieve strategic goals?
4. What role can SOF play in IO?
5. What role can IO play in special operations (SO)?
6. What impact will the integration of SOF and IO have on the on-going debate over roles and missions?
7. Should IO be a core SOF mission?
8. What IO capabilities do SOF currently possess and how are they utilized?
9. What IO capabilities should SOF possess to meet the strategic needs of the US?

D. FINDINGS

The findings of this thesis will assess the advantages of integrating SOF and IO and make recommendations on how to integrate these operations in order to maximize leverage and strategic utility. This integration will be examined from two perspectives: SOF as a supporting force and SOF as the supported force. It will also assess the current roles and missions of SOF and evaluate the propriety of IO as a primary SOF mission. The requirements generated by this integration will also be briefly examined.

E. METHODOLOGY

The methodology employed in this thesis will consist of the following:

1. Conduct a thorough literature survey and analyze different concepts of IO.
2. Review current joint and service doctrine, policy, and guidance on IO and SO.

3. Conduct interviews with relevant project officers and program managers responsible for conducting SO and IO.
4. Develop a conceptual framework for IO.
5. Examine the potential for integrating SOF and IO.
6. Examine the types of operations in which SOF and IO are being used together.
7. Examine the consequences of the integration on the future roles and missions of SOF.

This thesis will employ an inductive approach to developing a concept for the employment of SO and IO. I intend to use concept of "relative superiority" (from McRaven's Theory of Special Operations) and the decision cycle (the "OODA loop") as a departure point to examine how IO can create a window of opportunity and extend relative superiority.

F. ORGANIZATION

This thesis is composed of six chapters. This chapter provides the background, findings, and methodology employed to conduct the research. Chapter II presents a review of current literature and concepts of IO and IW and their strategic application. Chapter III examines the core competencies of SOF. It also explores how these competencies support strategic information operations. The integration of SOF and IO at the tactical level is explored in Chapter IV. It describes how information operations, by affecting the decision cycle, can open or extend the period of relative superiority in special operations. Chapter V examines the implications of these adaptations in the ongoing debate over roles and missions. Chapter VI provides a summary, conclusions, and recommendations for future research. Additional information about current DoD

definitions, computer security terms, SOF principal missions and collateral activities, and a compendium of various definitions of IO and IW is provided in four appendices.

II. INFORMATION OPERATIONS

For to win one hundred victories in one hundred battles is not the acme of skill. To subdue an enemy without fighting is the acme of skill.¹

Sun Tzu

The writings of the ancient Chinese strategist and philosopher, Sun Tzu, have received a great deal of attention in discussions of information operations (IO) and information warfare (IW). The preface of Samuel Griffith's translation of *The Art of War* offers a keen insight on the reason for Sun Tzu's current popularity:

Sun Tzu was well aware that combat involves a great deal more than the collision of armed men. 'Numbers alone', he said, 'confer no advantage.' He considered the moral, intellectual, and circumstantial elements of war to be more important than the physical, and cautioned kings and commanders not to place reliance on sheer military power.²

In a post-Cold War era of exploding information technology and growing asymmetric threats, even the overwhelming conventional military might of United States may not be sufficient to guarantee our security. Many people, including our adversaries, are looking to information and information technology for innovative ways to achieve strategic objectives. The terms "information warfare" and "information operations," and the concepts behind them, appear to some as the solution to this problem. They hold the potential to provide the United States a strategic advantage, possibly prevent conventional armed conflict, and reduce friendly (and perhaps enemy) casualties if armed conflict cannot be avoided. It is important to emphasize reducing casualties is not synonymous

¹ Sun Tzu. *The Art of War*, Trans. Samuel Griffith, (New York: Oxford, 1963) 77.

² Samuel L. Griffith. Introduction. Sun Tzu. *The Art of War*. Trans. Samuel Griffith, (New York: Oxford, 1963) x.

with eliminating casualties. The notion of bloodless conflict is, in all likelihood, a chimera. It is certainly not the position taken by the majority of IO advocates. Yet, reducing casualties with IO is a reasonable and attainable goal and represents the viewpoint of most IO optimists.

The topic is receiving attention at the highest levels of the U.S. government. Indeed, President Clinton used his commencement address to the 1998 graduates of the Naval Academy to stress the threat posed to the United States by "information warfare":

As we approach the 21st century, our foes have extended the fields of battle -- from physical space to cyberspace; from the world's vast bodies of water to the complex workings of our own human bodies. Rather than invading our beaches or launching bombers, these adversaries may attempt cyberattacks against our critical military systems and our economic base. ... Sometimes the terrorists and criminals act alone. But increasingly, they are interconnected, and sometimes supported by hostile countries.³

A scornful wit wrote that "two thirds of the earth's surface is covered by water, the other third is covered by papers on Information Warfare." The increased level of attention focused on this subject has served to highlight the contentious nature of the subject. Despite the generous attention this topic is receiving (or maybe because of it), there is a distinct lack of consensus; the same terms have different meanings for different people. They can encompass a diverse range of activities or a very narrow range, depending on the person speaking. Judging from the multitude of viewpoints and

³ William J Clinton, "Remarks at the United States Naval Academy Commencement" United States Naval Academy. Annapolis, Maryland, 22 May 1998.

accompanying terminology on information warfare and information operations, it seems that microprocessors are not the only subjects that adhere to Moore's Law.⁴

Martin Libicki compared determining the nature of information warfare to the attempts of three blind men to discover the nature of an elephant.⁵ Each participant could feel a small part of the elephant and declared it the nature of the whole, unknown object. Sorting out the competing visions and formulations for this emerging field is an important and necessary undertaking. Although there is still some disagreement on the exact definition and scope of IO, a common conceptual framework is essential to establishing any consensus on a definition. More importantly, establishing a common conceptual framework is necessary for strategy and policy formulation. According to Rand analyst Glenn Buchan:

The danger is that the way the problem is discussed can interfere--and indeed already has interfered--with the way the substantive issues are framed and analyzed, and that could lead to bad decisions that have unanticipated consequences.⁶

⁴ Gordon Moore was a co-founder of Intel Corporation. In 1965, while preparing a speech, he observed a striking trend. Each new chip contained roughly twice as much capacity as its predecessor, and each chip was released within 18-24 months of the previous chip. "Moore's Law" predicted that this trend would continue and the computing capacity of microprocessors would double every 12-18 months, leading to an exponential rise in computing power over relatively brief periods. "What is Moore's Law?" Online. Internet. Available: www.intel.com/intel/museum/25anniv/hof/moore.htm

⁵ Martin Libicki, *What is Information Warfare?* (Washington, D.C.: National Defense University Press, 1995) 3.

⁶ Glenn Buchan, *Information War and the Air Force: Wave of the Future? Current Fad?* Rand Issue Paper: Project Air Force. March 1996. n.pag. Online. Internet. Available: www.rand.org

This chapter will review and assess the different schools of thought on this subject and examine some of the essential issues surrounding them. The first section deals with terminology, specifically the IO vs. IW debate. The second section addresses the dispute about the novelty of information operations. The third section analyzes the details and implications of the different concepts of IO. The final section examines the strategic utility of the different concepts and offers a revised definition of information operations.

A. INFORMATION WARFARE VS. INFORMATION OPERATIONS

Is IO different from IW? The recent adoption of the term “information operations” signals a recognition of the fact that many people believe that the term “information warfare” is too restrictive. “Warfare” connotes open, armed conflict and leaves out operations conducted during peacetime and conflict short of war. It also excludes operations related to national security but conducted in cooperation with other government agencies outside of the DoD. Successful IO may well involve the participation of non-DoD organizations and activities, possibly including elements of the private sector. It is becoming increasingly clear that opportunities to use information for strategic advantage are not restricted to traditional battlefields. In fact, some view using information as a tool or weapon as a viable alternative to armed conflict. Author Winn Schwartau argues that

For the first time in history, the capability exists to wage a conflict (indeed a war) where no conventional munitions are required to achieve a stated goal; be that goal isolation, economic deactivation, sanctions or alternative to combat.⁷

Therefore, usage of the term "IO" generally constitutes an acknowledgement that information can be exploited for strategic advantage during peace, conflict or war by a variety of actors, not just the military. Under this convention, "information warfare" constitutes a subset of IO - the battlefield application of IO. This viewpoint is gaining currency; according to Department of Defense Directive S-3600.1 of 9 December 1996, information warfare is defined as "an *information operation* conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." (emphasis added)⁸ The U.S. Army has also adopted the term; FM 100-6, *Information Operations* states:

The Army, recognizing that IW as currently defined by DoD is more narrowly focused on the impact of information during actual conflict, has chosen to take a somewhat broader approach ... The Army adopted this approach to recognize that information issues permeate the full range of military operations (beyond just the traditional context of warfare) from peace through global war.⁹

For the reasons noted above, the broader term "information operations" is more appropriate when discussing the strategic use of information. Since many authors have yet

⁷ Qtd. in Robert D. Thrasher, *Information Warfare: Implications for Forging the Tools*, Thesis. Naval Postgraduate School, Monterey, June 1996, 27.

⁸ Quoted in Timothy L. Thomas, "The Mind Has No Firewall." *Parameters* Spring 1998: 85. DoD Directive TS-3600.1, *Information Warfare (IW)*, originally issued in December 1992, was replaced by DoD Directive S-3600.1 *Information Operations (IO)* on December 9, 1996.

to adopt this convention, the terms IO and IW will be used interchangeably, unless specifically noted.

B. INFORMATION-IN-WAR AND INFORMATION OPERATIONS

There is nothing new in recognizing information as a precious resource in warfare. The transmission of vital information was the purpose of the first marathon.

Lawrence Freedman

Many skeptics contend that information has always been important in conflicts. Indeed there are innumerable examples of information playing a critical and, in some cases, decisive role in conflicts throughout history. In *Cyberwar is Coming!* John Arquilla and David Ronfeldt cite examples from the Second Punic War and the Mongol conquests as proof that "information, communications, and control are enduring concerns of warfighters."¹⁰ More recent examples of the value of information abound, from the UTLRA project in World War II to the failed raid to capture Mohammed Farah Aideed in Somalia.¹¹ There can be no quibbling about the essential role of information in warfare.

The enduring value of information in war, though, is the basis for the most oft-raised objection to the concept of IO – that it is merely a new package for old concepts.

⁹ Department of the Army, *Field Manual 100-6, Information Operations* (Washington D.C.: Department of the Army, August 1996) 2-2.

¹⁰ John Arquilla and David Ronfeldt, *Cyberwar is Coming!* Reprinted in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: Rand, 1997) 32-37.

¹¹ Although the United States was not technically at war with Somalia, the operation to capture Aideed nonetheless constituted a combat action. The relief convoy's inability to navigate the streets of Mogadishu and locate the besieged raiders clearly demonstrated the critical nature of even elementary information.

Some of the objections raised¹² recall B.H. Liddell Hart's quip that "the only thing harder than getting a new idea into a military mind is to get the old one out."¹³ Undoubtedly, skepticism can be a healthy element in discussions of all aspects of IO. It is possible that the technological focus of much of the IO discussion may well bring forth the modern day equivalent of the Luddites¹⁴ but they are probably a minority; there is some legitimate skepticism. The question remains though, does IO merely represent the information age evolution of an ancient concept or is there something revolutionary about

¹² See R.L. DiNardo and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." and John Rothrock, "Information Warfare: Time for Some Constructive Skepticism?" DiNardo and Hughes offer a highly skeptical review of IW. They do present some compelling reasons for caution but some of their arguments are as specious as the ones they attack. They seem to be very fond of Clausewitz and Jomini while discounting the value of Sun Tzu. Particularly egregious is their suggestion that the writings of Sun Tzu are less valuable and sophisticated than Jomini and Clausewitz because they amount to "about 100 pages, as opposed to 600 pages of Clausewitz's writing and some 20 separate volumes published by Jomini." Equally derisive is their suggestion that fans of Sun Tzu "lack the patience to deal with the more sophisticated Clausewitz."

¹³ Quoted in Jay M. Shafritz, ed. *Words on War* (New York: Prentice Hall, 1990)256.

¹⁴ "People with an irrational and unfounded fear of that technology. In the early years of 19th century England revolution was in the air, the industrial revolution. This revolution was drastically reshaping the nation and impacting immensely on the world of work - especially in the textile trade, the work of artisans was now being done by machines. Enter Ned Ludd, a man of questionable mental ability, who managed to damage some of these new machines. Ned quickly drew a large following of artisans who expressed their dislike of the new technology by rioting and went on to destroy some newly invented mechanical looms because they thought such devices were going to deprive them of their livelihood. Their's (sic) was an irrational fear of technology, and the word Luddite continues to be applied with contempt to anyone with doubts about technology and its ability to solve most, if not all, of our problems." Ken Given, "Luddites, The RMA And Doctrine" Strategic And Defence Studies Centre (Australia). Online. Internet. Available: www.adfa.oz.au/DOD/dara/issue08.htm

IO? Simply put, IO is revolutionary only if results in significant changes in strategies, tactics, and organizations.

While revolutionary change has not yet occurred, a potential certainly exists and efforts are underway to effect these changes. Whether they will be successful is difficult to predict but Dan Kuehl suggests that three words distinguish current efforts to achieve revolutionary change: stovepipes, synergies, and integration.¹⁵ Many parochial activities (“stovepipes”), previously conducted with little or no coordination, are now being integrated and the combined effects of their coordinated application are synergistic. Much of the integration is the result of the application of network technologies to share information. This integration should result in organizational changes and present the opportunity for strategic and operational innovation.

Much of the skepticism regarding IO is the result of two factors: confusing the application of information technology with IO and failing to distinguish between the importance of information in war and the concepts of information operations. The traditional role of information in war has been to provide the battlefield commander with knowledge of battlefield conditions – friendly and enemy location, strength, movements, weather, terrain, etc.– and possibly to mislead the enemy about the friendly situation. Martin van Creveld states:

¹⁵ Dan Kuehl, “Defining Information Power.” *Strategic Forum* Number 115, June 1997. n.pag. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum

From Plato to NATO, the history of command in war consists essentially of an endless quest for certainty – certainty about the state and intentions of the enemy's forces; certainty about the manifold factors that together constitute the environment in which the war is fought, from the weather and the terrain to radioactivity and the presence of chemical warfare agents; and, last but definitely not least, certainty about the state, intentions, and activities of one's own forces.¹⁶

This allowed the commander with better information to gain the initiative – to choose the time and place of an engagement and defeat the enemy forces. In contrast to the other services, the US Air Force has recognized this fact and offers a definition of “information in war”:

Information-in-war involves the AF's extensive capabilities to provide global awareness throughout the range of military operations based on integrated intelligence, surveillance, and reconnaissance (ISR) assets; information collection/dissemination activities; and global navigation and positioning; weather; and communications capabilities.¹⁷

Additionally, the traditional focus of war has been on physical destruction, whether of the enemy himself or his capacity to make war. Some of the current discussion of IO/IW concerns integrating information technology with the existing paradigm of war – a paradigm defined by Clausewitz and Jomini. This paradigm assumes that states make war and focuses on the physical destruction of the enemy force and the enemy's will to resist. It seems clear that these assumptions are not always valid in the current environment. Non-state actors are increasingly capable of confronting states with asymmetric strategies designed to avoid the dominance of the state on the traditional

¹⁶ Martin van Creveld, *Command in War* (Cambridge: Harvard University Press, 1985) 264.

¹⁷ Department of the Air Force, *AFDD 2-5: Information Operations* (Washington, D.C.: Department of the Air Force, 5 August 1998) 2.

battlefield. Additionally, as the Zapatista "Netwar" in Mexico has demonstrated, it is not necessary to destroy an adversary in order to achieve strategic objectives.¹⁸

Many of the discussions regarding IO and IW also automatically include anything involving information technology (IT). C. Kenneth Allard argues that "one of the major legacies of Desert Storm will be the continuing effort by the U.S. defense establishment to exploit the potential of advanced technology and precision weaponry in an emerging paradigm of information warfare."¹⁹ The most potent example is the issue of "digitizing the battlefield," which refers to efforts to integrate advanced IT into existing systems and to incorporate it in new systems. The US Army has conducted a series of "advanced warfighting experiments" to explore the potential for applying these concepts. The hypothesis is that a digitized force, with properly integrated technologies and doctrine, will possess increased lethality and survivability, and operate at a higher tempo.²⁰ The ultimate goal is to provide US forces with the "information dominance" identified in *Joint Vision 2010*:

¹⁸ David Ronfeldt and Armando Martinez. "A Comment on the Zapatista Netwar." In *Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds. (Santa Monica: Rand, 1997) 369-391.

¹⁹ C. Kenneth Allard, "The Future of Command and Control: Toward a Paradigm of Information Warfare" in *Turning Point: The Gulf War and U.S. Military Strategy*, L. Benjamin Ederington and Michael J. Mazarr, eds. (San Francisco: Westview Press, 1995) 161.

²⁰ US Army Training and Doctrine Command, "Force XXI Hypothesis" Briefing. Online. Internet. Available: www-tradoc.army.mil/pao/awel.htm

The digitized battlefield is the linchpin of the Army's Force XXI vision, allowing seamless C2 from the Corps commander to the soldier in the foxhole. Inherent in this vision is the need to gain and maintain information dominance, which gives Army commanders the ability to access the information required to synchronize battlefield actions.²¹

Much of this is merely improvement to existing platforms with the immediate goal of providing better management of information – vertically and horizontally integrated battlefield communications that enhance situational awareness and engagement capabilities on the battlefield. There has been little doctrinal or organizational innovation. The concept of precision engagement, as applied here, still implies the physical destruction of a target. Other related concepts include “dominant battlefield knowledge” or “dominant battlespace awareness.”²² The US Navy refers to its version of these concepts as “network centric warfare,” which is being implemented through the Information Technology for the 21st Century (IT-21) strategy.²³ Despite claims of innovation, these efforts are focused (explicitly or not) on enhancing existing command, control, communications, and intelligence (C3I).

As Ronald J. Knecht observes, “Achieving more efficient and effective information operations than a potential adversary is a sound goal; it just should not be

²¹ Air Land Sea Application Center, *Information Warfare/Information Operations Study*, 15 December 1995, p.8-10.

²² For a detailed discussion of these concepts, see Martin Libicki and Stuart Johnson, eds. *Dominant Battlespace Knowledge*, (Washington D.C.: NDU Press, October 1995).

²³ Department of the Navy, “What is IT-21?” n.pag. Online. Internet. Available: www.inpo.navy.mil/it-21/it-21.html

labeled information warfare.”²⁴ Unfortunately, some influential publications contain definitions that do just that. This confusion is reflected in the definition of IO found in the US Army Field Manual 100-6:

Information operations are continuous military operations within the military environment that **enable, enhance, and protect the friendly forces ability to collect, process, and act on information to achieve an advantage** across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities. (emphasis added)²⁵

Additionally, *Joint Vision 2010* declares “We must have 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.”²⁶ It is obvious that the vision of the Army and the Joint Chiefs is primarily geared towards better management of information on the battlefield.

These discussions place information operations “in the role of combat support rather than as a new form of combat proper.”²⁷ Information is viewed as an enabler of

²⁴ Ronald J. Knecht, “Thoughts on Information Warfare” in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds. (Fairfax: AFCEA International Press, 1996).161. The terminology problem noted earlier seems to be quite evident here. I believe that Knecht uses “information operations” here in a generic sense (i.e.-gathering and processing information or data), not in the context of a larger umbrella for IW discussed in the previous section.

²⁵ Department of the Army, *FM 100-6*, 2-3.

²⁶ Department of Defense, *Joint Vision 2010*, (Washington, D.C.: Dept. of Defense, 1996) 16.

²⁷ George J. Stein, “Information Attack: Information Warfare in 2025.” *Air Force 2025* Vol.3, Book 1. (Maxwell AFB: Air University. August 1996) 11.

combat, not as a weapon or target in its own right. Yet, proponents of IO believe that the proliferation of IT and the growing dependence on it have created new vulnerabilities and opened the door to the possibility of information as both a weapon and a target. Lawrence Freedman observes:

Though the importance of increasing one's own knowledge while limiting the enemy's has long been realized, it has historically been ancillary to other operations. Something has changed which allows us to consider information warfare in a new, more comprehensive light. That something is the proliferation, increasing sophistication, and growing connectivity of modern information systems. This has created a situation where, for the first time, an information realm exists within which we can conduct widespread military operations.²⁸

Other revolutions in military affairs (RMAs) have resulted in a more efficient destruction of the enemy. They changed the strategy, tactics, and organization but still focused on attrition or annihilation of the adversary. Does this RMA have to be any different? No, it doesn't (and maybe it won't be) but it does hold the possibility for a more radical transformation – a shift in focus from the physical realm to the information realm where information is both a weapon and a target. To focus on improving traditional means of warfare through the employment of IT ignores the enormous strategic potential offered by IO. The potential exists that we may yet achieve the “acme of skill.”

Improving current capabilities with sophisticated technologies, while it may be beneficial in some regards, is also potentially dangerous and counterproductive. “Advanced information and communication systems, properly applied, can improve the

²⁸ Lawrence Freedman, “Information Warfare: Will Battle Ever be Joined?” Lecture. International Centre for Security Analysis (ICSA), London. 14 October, 1996. n.pag. Online. Internet. Available: www.Infowar.Com/mil_c4i/icsa/icsa1.html-ssi

efficiency of many kinds of activities. But improved efficiency is not the only or even the best possible effect” according to John Arquilla and David Ronfeldt.²⁹ Granted, the potential offered by IO is unfulfilled, but the opportunity cost of ignoring it is potentially very high. Further pursuing improvements to our conventional capabilities, many of which are very expensive, may lessen the chances of a conventional conflict but it introduces considerable risks. As Arquilla points out in a recent article in the *World Policy Journal*:

For the U.S. military, simply grafting new weapons onto the existing organizational structures may ultimately lead to greater vulnerability, as potential adversaries will no doubt acquire advanced technologies and may also create new, nimble units that are much less easily targeted than the American military’s heavy divisions, air wings, and naval battle groups.³⁰

Arquilla advances the proposition that “the pursuit of radical advances [in conventional capabilities] might actually lead to the erosion of the current position of relative advantage.”³¹ The United States currently enjoys a considerable advantage in conventional capabilities. The size of this advantage and the costs of overcoming it create a considerable disincentive for direct competition with the United States; few adversaries appear able or determined to challenge the U.S. directly. While we spend time and money on improving our advantage, many of our potential adversaries are searching for innovative and asymmetric strategies, which may render our current advantage moot.

²⁹ Arquilla and Ronfeldt, *Cyberwar* 26.

³⁰ Arquilla, John, “The “Velvet” Revolution in Military Affairs.” *World Policy Journal*. Winter 1997/98, Vol. XIV, No. 4: 33.

³¹ Arquilla, “Velvet” 34.

Therefore, an immediate threat may result from devoting scarce fiscal resources to areas in which we enjoy significant advantages at the cost of training and readiness.³²

Of course, this dynamic of innovation and counter-innovation has historical precedent but the cost and significant vulnerabilities of many advanced technologies should give us pause. For example, many of the new technologies are "commercial-off-the-shelf" (COTS) items that are not hardened against electromagnetic pulses (EMP). The U.S Army's Force XXI concept is decidedly vulnerable to this threat.³³ Difficulties in preventing the proliferation of nuclear technologies, as evidenced by the recent events on the Asian subcontinent, make this a viable threat.³⁴ CIA Director John Deutch, testifying before the Senate Permanent Subcommittee on Investigations, stated: "The chilling reality is that nuclear materials and technologies are more accessible now than at any time in history."³⁵

We should separate our attempts at improving the efficiency of our own communications and information management in traditional conflict from the concept of

³² Arquilla, "Velvet" 39.

³³ Sean J. A. Edwards, "The Threat of High Altitude Electromagnetic Pulse to Force XXI." *National Security Studies Quarterly* Autumn 1997, Vol. III, Issue 4: 61-79.

³⁴ On May 11 and 13, 1998 India exploded an undetermined number of nuclear devices in underground tunnels. The underground test came as a surprise to U.S. intelligence agencies. Pakistan responded on May 28, 1998 by detonating five nuclear devices. *Chronology of the India-Pakistan Conflict*. New Delhi: Reuters News Service, July 26, 1998. Online. Internet. Available: www.napf.org/asia/indiapakchron.html

³⁵ Quoted in Webster, William, et. al., *The Nuclear Black Market*. (Washington, D.C.: Center for Strategic and International Studies, 1996) 1.

IO.³⁶ While IO is certainly enabled by advances in technology and increasing dependence on information, it is a mistake to place every application of IT under the IO umbrella. Information technologies are being applied rapidly to every aspect of society – social, political, economic, and military; in its multitude of forms, IT is becoming ubiquitous. Subsuming all applications of IT under IO would render the concept meaningless.

The objective of many of these applications is a more efficient platform-based force, a force focused on the physical destruction of the adversary. Using IT to improve our conventional warfighting capability, planning to fight the last war with the latest technology, is merely evolutionary, not revolutionary. This approach still views information in a supporting role for physical combat rather than a realm of warfare unto itself. The ability to physically destroy an enemy on the battlefield will undoubtedly endure. However, IO should seek to reduce this requirement before the battle is joined.

My intent is not to debate whether we are truly in the midst of an RMA but merely to point out that simply embedding improved IT in our existing platforms and capabilities is not, in itself, revolutionary. The bottom line answer is that if we believe that IO is a truly revolutionary concept, IT used to improve battlefield information management (the collection, processing, and distribution of information) should not be considered part of IO. Accepting the distinction between information in war and IO has a significant impact

³⁶ It is important to distinguish between improving efficiency and improving security and survivability. While all three are important goals, the latter two may be essential as defensive measures against adversary information operations. The former may be more important on a traditional battlefield. It may very well be that new systems incorporate improvement in all three areas but there is not a direct correlation between

on the IO debate, effectively removing digitization of the battlefield from discussions. As George Stein of the Air War College states unequivocally that "Whether we are digitizing the cockpit or digitizing the battlefield, this is not IW."³⁷

C. CONCEPTS OF INFORMATION OPERATIONS

Anybody who makes more than \$5 an hour and works on this side of the Mississippi has tried to define Information Warfare.

Dan Kuehl, National Defense University

There are those who believe (or at least say they do) that no definition is necessary or possible; any attempt at definition risks limiting our horizons and achieving consensus is hopelessly difficult. Martin Libicki, formerly of the National Defense University and now at Rand, argues that "Information warfare, as a separate technique of waging war, does not exist." Rather, he argues there are seven distinct forms of information warfare, which are at best weakly related.³⁸ He derides the concept of IW as lacking any analytic coherence. Similarly, John Rothrock writes:

these three elements. Because there is not a direct correlation it is possible (though maybe not always desirable) to address these issues independently.

³⁷ Stein, 11.

³⁸ Libicki, *Information Warfare* 7. The seven forms of Information Warfare identified by Libicki are command-and-control warfare (C2W), intelligence-based warfare (IBW), electronic warfare (EW), psychological warfare (PSYW), hacker warfare, economic information warfare (EIW), and cyberwarfare.

Today, when one reads about information warfare and hears the concept in presentations, it remains very difficult to determine if there is anything that Information Warfare is not. A skeptical mind is soon prompted to ask, "*If Information Warfare is everything, can it be anything?*" (emphasis original)³⁹

These criticisms are not completely unfounded and Libicki may be correct, for now. Many disparate elements are frequently lumped together as "information warfare" in sweeping definitions far too broad to have much analytic value. Libicki repeats a definition offered by the late Thomas Rona:

The strategic, operational, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.⁴⁰

Rona, an early proponent of IW, is definitely not alone in offering an indiscriminate definition of IW. For example, the Secretary of the Air Force Sheila Widnall and USAF Chief of Staff Ronald Fogleman declared "Information warfare is any attack against an information function, regardless of means...Information warfare is any action to protect our information functions, regardless of means."⁴¹ They assert that bombing a telephone switch or defending a switch from air attack both constitute information warfare. It is indeed difficult to see how such broad definitions can lend themselves to useful policy or strategy decisions.

³⁹ John Rothrock, "Information Warfare: Time for Some Constructive Skepticism?" in *Athena's Camp: Preparing for Conflict in the Information Age*, John Arquilla and David Ronfeldt, eds. (Santa Monica: Rand, 1997) 220.

⁴⁰ Libicki, *Information Warfare* 4.

⁴¹ Department of the Air Force, *Cornerstones of Information Warfare* (Washington D.C.: Department of the Air Force, 1996) n.pag.

There is little in the way of a large-scale, coordinated effort to plan and conduct IO. Each service and government agency has its own conception of IO and there is no joint doctrine for IO within DoD (although a draft publication, Joint Publication 3-13, *Joint Doctrine for Information Operations*, is currently being staffed). Significant hurdles await any attempt to craft a national information strategy or an interagency effort on IO.

Despite these obstacles, it is necessary to forge ahead in exploring the potential of IO and recall that concepts like strategic airpower and armored warfare were not developed overnight. They too faced significant opposition and years of experimentation to fulfill their promise:

Sometimes the vision of the innovators has outrun the capability of technology: the early submariners, the early aircraft carrier advocates, the first air power theorists, the proponents of surface-to-air missiles, and, just possibly, those enthusiasts who unreservedly espouse the cause of enhanced technology as the panacea for today's Western strategic dilemmas might be so categorized. Yet, without such visionaries and without innovation, a nation's way of war becomes predictable; and predictable means vulnerable.⁴²

A well-crafted definition and the common vocabulary that accompany it are necessary to facilitate the difficult decisions on policy, organization, and strategy that will allow IO to fulfill its promise.

While there are indeed many different definitions of IO and IW, there are far fewer core concepts. It would be difficult, if not impossible, to catalog the particulars of every definition. However, the competing IO definitions can be categorized by their overall approach and emphasis: infrastructure or psychological.

The first approaches IO from a technical perspective, placing a primary emphasis on disrupting and protecting information systems and processes. The second approaches IO from a psychological perspective, placing the emphasis on managing and manipulating perceptions or creating a "fictive" reality. A third category is comprised of definitions that do not fit well in either the first or the second category but usually combine aspects of the other two concepts in an all-encompassing approach. A common theme, albeit with lesser emphasis, which is found in all three categories is the defensive component of IO.

1. Information Systems Approach

This approach targets the information systems and processes of an adversary. The focus is on destroying or disrupting the systems in order to take away the adversary's means to react or resist. The goal is to make the attacks so devastating that the adversary will have few options other than to consent to the attackers' demands. According to Lawrence Freedman:

The enthusiasts for strategic information warfare are looking well beyond the old intelligence game. They have identified information systems as being so important to both the military and society in general that together they constitute a critical dependency. We would prefer to avoid the pain, heartache and mess associated with actually eliminating or destroying an enemy by instead rendering him incapable, and it is possible this should be achieved using means that involve only a minimum of risk to your own armed forces.⁴³

⁴² R. A. Mason, "Innovation and the Military Mind." *Air University Review* January-February 1986. n.pag.

⁴³ Freedman, n.pag.

In general, the critical infrastructure of the adversary and its supporting systems are the targets of this approach. The President's Commission on Critical Infrastructure protection (PCCIP) identified five categories of critical infrastructure: information, banking and finance, energy, physical distribution, and vital human services. These categories are very general and applicable to most societies although the degree of dependence may vary substantially. The table below identifies some of the major elements of each category:

Table 2-1: Critical Infrastructure Categories and Elements⁴⁴

Critical Infrastructure Category	Major Infrastructure Elements
Information	Telecommunications (e.g. public telephone network) Computer networks Media services
Banking and Finance	Stock and financial markets Commodities markets Banking and credit Investment institutions Exchange boards, trading houses, reserve systems
Energy	Raw material production and storage Power production and distribution
Physical Distribution	Water supply and sewage treatment Oil and gas pipelines Highways and rail lines Airports and airways Mass transit systems
Vital Human Services	Basic government services Emergency services National security services Education Health care Public safety/law enforcement

Where the adversaries are states, this may be the national or military infrastructure. Where the adversary is a non-state or sub-state actor, it may be portions of the global or national information infrastructure upon which those entities depend. Infrastructure in this concept is not necessarily limited to the physical components of information systems; it may also include the human component of these systems, e.g. – programmers, operators, technicians. This approach also targets the software components of information systems.

⁴⁴ Edward Waltz, *Information Warfare: Principles and Operations* (Boston: Artech House, 1998) 179-180.

While Freedman and others focuses on the application of this approach by a state it must be noted that "information terrorists" or "cyberterrorists" could also attempt to employ this approach, or smaller well-targeted attacks, in lieu of or as an adjunct to traditional armed attacks.⁴⁵ One possible, and probably the most publicized, threat posed by this type of information operation has been likened to an "electronic Pearl Harbor."⁴⁶ Typically, this scenario envisions "a massive attack on the military and governmental (command and control) information infrastructures, with perhaps collateral attack against important civilian networks that aid and support military, governmental, and social stability."⁴⁷ This attack would constitute a preemptive strike in an attempt to force acceptance of the aggressor's demand by crippling the information dependent functions of the target. A similar, less apocalyptic scenario is dramatized in John Arquilla's short story

⁴⁵ For more information on this subject see Mathew J. Littleton, *Information Age Terrorism: Toward Cyberterror*. Thesis. Naval Postgraduate School, Monterey, December 1995.

⁴⁶ A much more useful metaphor for this approach may be an "Information Hiroshima." The attack on Pearl Harbor, though swift and brutal, was obviously not a permanent setback and it did not cripple the United States or force it to accede to Japan's demands. Additionally, the operational means employed in the attack were not revolutionary. Finally, there is no information-age equivalent to "battleship row" a single physical location in which a great deal of national power is concentrated. Networks and information systems are distributed systems and inherently robust. All this is in contrast to the use of nuclear weapons against Japan (undoubtedly a revolutionary development) which led to an immediate and unconditional surrender. The Pearl Harbor analogy is useful in illustrating the potential for strategic information operations to delay a U.S. response to an attack, on the U.S. itself or a third party. This strategic paralysis could allow an adversary to complete a *fait accompli*. Conversely, it is also a cautionary tale: while the attack did impede the US ability to stop the Japanese advances, it also served to harden the national will and guaranteed that the U.S. would respond with its full military might.

"The Great Cyberwar of 2002." In some regards, this approach is command and control warfare (C2W) writ large; the infrastructure necessary for maintaining societal order and control is crippled or destroyed.⁴⁸

There are two primary methods to conducting this attack: denial of service and violation of integrity. Denial of service limits the availability of information or information systems upon which essential services depend. Violation of integrity alters or corrupts the information required to render essential services; false information may be propagated to confuse or deceive information systems. These services can be social, economic, military, or governmental in nature but must have some information or information system dependency.

This approach appears to be the dominant perspective within the Department of Defense. According to Department of Defense Directive S-3600.1 of 9 December 1996, an information operation is defined as "actions taken to affect adversary information and information systems while defending one's own information and information systems."⁴⁹ An identical definition is found in the final draft of Joint Publication 3-13, *Joint Doctrine for Information Operations*. The most recent DoD Joint Dictionary defines information operations as:

⁴⁷ Michael Wilson, "Battle for the Soul of Information Warfare: Pearl Harbor vs. The Hashishim." 1996. n.pag. Online. Internet. Available: www.7pillars.com/papers. 31.

⁴⁸ C2W is considered the *military* application of IW. In many ways, the infrastructure concept of IO is similar to C2W on a societal scale. Please refer to the glossary in Appendix A for the full definition from *DOD Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*.

⁴⁹ Quoted in Thomas, "Firewall," 85.

Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW.⁵⁰

Likewise, the US Army defines information warfare as "actions taken to achieve information superiority by affecting a hostile forces' information, information based-processes, and information systems, while defending one's own information, information processes, and information systems."⁵¹ Ronald J. Knecht offers a slightly different formulation: "The preparation for and use of physical and logic-based weapons that disrupt or destroy information or information systems in order to degrade or disrupt information function(s) that depend on the information and information systems." Knecht also points out that the DoD definition focuses on achieving an unspecified level of "information superiority" while his definition focuses on "the functions that depend upon information systems, not the supporting infrastructure."⁵²

A variety of different means is available to deny services. Of course, the physical destruction of a system is a time-honored method for preventing its use but this method is generally restricted to open hostilities. Attacking in the physical realm is anathema to some "true information warriors." According to Winn Schwartau:

⁵⁰ Department of Defense, *DOD Joint Publication 1-02 Dictionary of Military and Associated Terms*. n.pag. Online. Internet. Available: www.dtic.mil/doctrine/jel/doddict/

⁵¹ Department of the Army, *Field Manual 101-5-1, Operational Terms and Graphics*, (Dept. of the Army: Washington D.C., 1997) 1-82.

⁵² Knecht 165.

Simply, any IW definition that requires military involvement, in my humble opinion, is self-limiting. You just don't need bombs and bullets for the kinds of IW I have postulated and described to be effective. In fact, bombs and bullets can be considered anathema to effective IW.⁵³

Other more subtle methods are available that generally hew closer to the IO ideal articulated by Sun Tzu: achieving victory without armed battle.⁵⁴ At one end of the spectrum may be attacks that merely inconvenience information system users, such as Robert Morris's infamous Internet "worm."⁵⁵ This simple program exploited known weaknesses in an operating system to distribute itself and consume resources on the host computer. Authorized users were denied services when the "worm" had consumed all of the available resources. At the other end of the spectrum are attacks that interfere with a vital ability of the adversary, such as the capacity to deploy forces quickly in a crisis. For example, a possible target could be the air traffic control system or the automated system that the US Air Force uses to determine Air Tasking Orders (ATO). Attacks on these targets would not be merely annoying but could pose a real threat to national security or public safety. The possibility also exists for extending these attacks to space and disabling space based intelligence or communications platforms. In all of these cases, the result is essentially the same: an essential service is unavailable.

⁵³ Electronic mail posting to C4I-Pro Forum. n.pag. Online. Internet. 28 Nov 1995. www.stl.nps.navy.mil:80/lists/c4i-pro/#end.

⁵⁴ A more practical goal is the habitual integration of IO and conventional forces. This integration would be characterized by the recognition that IO can enhance the effectiveness of conventional forces and vice versa.

⁵⁵ See Littleton, 86-90.

A denial of service attack could be directed against public telephone networks. Service could also be denied by feeding false or misleading information that causes the system to malfunction. With computer networks this could be accomplished using malicious software, in the form of viruses or "Trojan horses," or by hackers gaining unauthorized access. Attacks of these types, whether using malicious software or gaining unauthorized access, are generally classified as "computer network attack" (CNA).

In addition to CNA, electronic warfare (EW) is also useful for denial of service attacks. EW includes jamming, electromagnetic deception, and "employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams)."⁵⁶ Directed-energy weapons, such as high-energy radio frequency (HERF) guns, can permanently disable many electronic devices. HERF guns aim high-energy radio frequencies at a specific target, overloading and disabling – temporarily or permanently – its communications, computer, and other electronic equipment. The HERF gun takes advantage of the microprocessor's sensitivity to high levels of energy and essentially cause the integrated circuits to overload and burn out. As microprocessors become ubiquitous, the number of potential targets becomes enormous. The HERF gun may be used in wartime to disrupt communications, interfere with enemy aircraft's avionics, and cause malfunctions in ground-based transportation.

Another possibility involves the uses of an electromagnetic pulse to disable sensitive electronic components. This is perhaps the most popular and intriguing of new weapons technologies. It involves the harnessing of an electromagnetic pulse, which may

couple with electrical/electronic systems to produce damaging current and voltage surges. Although this phenomenon is most frequently associated with nuclear explosions, it is possible to generate a similar effect using conventional explosions. Although some of the technology is mature, the output generated by conventional explosives is restricted to frequencies less than 1Mhz. Because of the low frequency, higher power levels are required to achieve the desired effects. Additionally, it is difficult to focus the output from such a weapon. It destroys the electronics of all computer and communication systems in a quite large area. High power microwave (HPM) systems present a possible alternative. Because of the high frequency and greater directional capability, the directed energy may couple more easily to achieve the desired effects.⁵⁷ A critical limitation on both of these systems is portability due to power requirements; they are large and bulky, which restricts the means of employment.

While directed energy weapons hold the potential for covert use in peacetime as well as in war, they are still in the developmental stage. This fact is the basis for some legitimate skepticism. One author has gone so far as to label EMP guns "the Chupacabras of Infowar," a derogatory reference to the mythical blood sucking beast that terrorizes Latin America.⁵⁸ While this is obviously hyperbole, the fact is that there is probably a

⁵⁶ DOD, *Joint Pub 1-02*, n.pag.

⁵⁷ Carlo Kopp, *The Electromagnetic Bomb – A Weapon of Electrical Mass Destruction*. n.pub. Online. Internet. Available: www.hut.fi/~zam/ew/mirror/apjemp.html.

⁵⁸ George Smith, "EMP Gun: The Chupacabras of Infowar," *Netly News* July 22, 1997. Online. Internet. Available: www.soci.niu.edu/~crypt/other/chupax.html.

long way to go before these phenomena are effectively weaponized for use by ground forces.

Defending against denial of service attacks is generally referred to as “information assurance”; it can include physical security, operational security, and counterintelligence.⁵⁹ Physical security includes not only access controls but may also include structural defenses such as hardening or shielding systems from electromagnetic pulses or directed energy weapons. This not an easy task. As the number and type of information systems increases, it becomes harder to identify and address all possible vulnerabilities. For computer networks, firewalls and anti-virus software can address part of the problem. While cryptography is very useful for ensuring the confidentiality and integrity of information, it has limited value in ensuring system availability. It can support authentication policies but does not protect against malicious software or directed energy weapons. In most cases, the weakest link will be the human interface with the information system.⁶⁰

The utility of this approach is directly proportional to an adversary’s dependence on information systems. The level of dependency and the criticality of the service primarily determine the efficacy of this type of attack. Other factors that could affect the outcome of this type of attack are the duration and intensity of the attack. It is not always

⁵⁹ Please refer to the glossary in Appendix A for the full definition.

⁶⁰ Cited in *Forbes Digital Tool*, n.pag. 10 Oct 1997. Online. Internet. Available: www.forbes.com/tool/html/97/oct/1010/colb.htm. The Computer Security Institute’s 1997 Computer Crime and Security Survey found that employers suspected disgruntled employees in 80 percent of attacks and that the single largest method of attack was through unauthorized access by an insider.

necessary, desirable, or possible, to disable a system completely and permanently. It may be possible to achieve the desired effects by simply slowing a system down. This may be beneficial in that an adversary may not recognize the attack and actions to restore service may be delayed. Additionally, obvious attacks may only be effective against a particular system once; if the adversary is able to determine the vulnerability, he may take corrective action, which precludes this type of attack in the future. Further, the rapid pace of technological change may render some methods of attack useless as security features are improved and vulnerabilities eliminated. This is not to say that systems will become completely secure but only that new systems will likely have different vulnerabilities that must be identified by would-be attackers.

A significant shortcoming of this approach is the inability to affect less advanced adversaries. Adversaries, whether states or some form of non-states actors, that are not dependent upon information technology are much less susceptible to this type of approach. Another possibility is that the adversary's capabilities may be "nested" in the information infrastructure of a friend or ally. It may be difficult to target the adversary's systems without causing collateral damage.

With regard to malicious software, particularly viruses, some troubling questions remain about their utility for military operations. First, the complexity and heterogeneity of computer makes it difficult to anticipate the type of system the virus will encounter. Developing system specific viruses requires skilled software writers and increases the demands on the intelligence community for detailed information about a system. Second, viruses are not precision guided munitions; they can spread rapidly and indiscriminately,

damaging friend and foe alike. Third, truly catastrophic viruses are likely to be a wasting asset; once discovered, some form of immunity will ultimately develop.⁶¹

Another potential problem with this approach is that it is unclear whether this approach could really achieve the desired strategic results. Several factors contribute to this uncertainty. First, many "information systems" are networks that are, in general, very robust. Even if some portions of the network are destroyed, other portions may still be able to function because of redundant architectures with multiple paths. Second, it may be difficult to determine exactly which portions of a system are the most critical. As Lawrence Freedman points out:

[T]he multiplication of channels through which information can pass both reduces dependence upon a single channel but also the opportunities to control the flow. There are few information 'choke points', no 'command of info-power' easily obtained, no 'centre of gravity' to be targeted.⁶²

There may also be more primitive backup systems, which restore a certain level of functionality to the overall system. These backups may not be as vulnerable to this type of attack as the primary systems. There is also the danger of unintended consequences: an adversary subject to this type of attack (or who merely believes that he is under attack) may not react in predictable ways. The threat of unintended consequences takes on added

⁶¹ George Smith, "An Electronic Pearl Harbor? Not Likely," *Issues in Science and Technology Online* Fall 1998. n.pag. Online. Internet. Available: www.nap.edu/issues/15.1/smith.htm

⁶² Freedman n.pag.

significance when we consider that the Russians have publicly discussed using nuclear weapons in response to an information attack.⁶³

Finally, there is little or no evidence yet that denying the use of information or information systems can destroy or undermine the will to resist. While this is certainly a theoretical possibility it has yet to be proven by practical application. Even if an attack succeeds in crippling major information systems, the attacker will, still need, in all likelihood, some credible threat of force to achieve complete victory. It is useful to remember the resilience displayed by citizens of Leningrad; if human beings can endure this type of siege, it is difficult to imagine the lack of availability of information systems bringing them to their knees.⁶⁴

None of this should be construed as arguing that this approach is worthless or unrealistic. Rather, it means that it is important for us to recognize that there are some limitations to what can be achieved and to carefully consider how this approach supports our strategic objectives. As Glenn Buchan writes:

⁶³ Timothy L. Thomas, "Russian Views On Information-Based Warfare," *Air Power Journal* July 1996 Special Edition: 26.

⁶⁴ For a full description see Harrison Evans Salisbury, *The 900 Days: The Siege of Leningrad* (New York: Da Capo Press, 1985).

There is a danger that the trendiness of attacking information systems will cause people to lose sight of the fact that such operations, like any others, must serve particular military and political objectives and may have to compete with other missions for priority and resources. The difficulties with predicting the effects of such attacks have always been an issue, and the traditional intelligence problems of identifying suitable vulnerabilities and determining the best ways to execute such attacks are likely to become even more formidable in the future. Also, Sun Tzu notwithstanding, denying an enemy the use of information is not always a particularly wise idea. ... Probably an ideal objective would be to control the information adversaries have and which of their information-related systems continue to function.⁶⁵

2. The Psychological Approach

This approach focuses primarily on the subtle manipulation of the decision-making processes of an adversary. The immediate goal is influencing, or possibly even controlling, the adversary by managing or manipulating perceptions. The ultimate goal is to cause the adversary to make decisions and act upon them in ways that will support friendly strategic objectives (behavior modification). In contrast to the infrastructure approach, the will of the adversary is not necessarily crushed but rather it is altered. Ideally, all of this would be accomplished in such a way that the adversary was unaware of any attempt to influence him and achieve the desired strategic objective with or no use of force.

This approach differs from the infrastructure approach in that it seeks to employ more subtle methods; information systems, instead of being the target, provide a pathway to the target. In general, the mind or thought process of the adversary is the target of this approach. The target may be the collective "mind" of a target population or community

⁶⁵ Buchanan, pag.

but most advocates envision a more selective target audience, e.g. the thought processes of an individual decision-maker. Arquilla and Ronfeldt label this approach as "Netwar":

Netwar refers to an information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movement across computer networks.⁶⁶

This approach is more concerned with psychological domination than destroying or impairing information infrastructures. It is important to understand that the infrastructure may be targeted in support of the ultimate objective, but that these attacks must contribute to influencing the target audience, not merely creating mayhem. The approach of Colonel Richard Szafranski embodies this concept:

Information warfare is waged against the epistemology, the entire structure and beliefs, of an adversary. ...The object of information warfare...is to subdue hostile will utterly, but without, or with little, physical fighting. The target sets of information warfare are the minds of adversary leaders and adversary citizens.⁶⁷

Szafranski also promotes the notion of "neocortical warfare," referring to the neocortex, that portion of the human brain which "enables us to think, organize, remember, perceive, choose, create, imagine and cope with or adapt to novelty." He defines this as:

⁶⁶ John Arquilla and David Ronfeldt, *Cyberwar* 28.

⁶⁷ Richard Szafranski, "An Information Warfare SIIOP." n.pag. Online. Internet. Available: www.infowar.com/mil_c4i/szafran.html-ssi

[W]arfare that strives to control or shape the behavior of enemy organisms, but without destroying the organisms. It does this by influencing, even to the point of regulating, the consciousness, perceptions and will of the adversary's leadership: the enemy's neocortical system. In simple ways, neo-cortical warfare attempts to penetrate adversaries' recurring and simultaneous cycles of 'observation, orientation, decision and action.'⁶⁸

George Stein takes a similar view:

Information warfare, in its essence, is about *ideas and epistemology* – big words meaning that information warfare is about the way humans think and, more important, the way humans make decisions. And although information warfare would be waged largely, but not entirely, through the communications nets of a society or its military, it is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decisions they make.⁶⁹

How is this form of IO different from traditional propaganda, psychological operations, and deception? At first glance, this approach would seem to differ little from traditional notions of these three related disciplines.⁷⁰ One difference is the integration of these separate discipline sought by IO advocates. Arquilla and Ronfeldt note that “designing a strategy for Netwar may mean grouping together from a new perspective a number of measures that have been used before but were viewed separately.”⁷¹ Another difference is the degree to which IO influences the target audience. Stein addresses the comparison with propaganda directly:

⁶⁸ Richard Szafranski, “Neocortical Warfare? The Acme of Skill.” *Military Review* Vol. 74, no. 11 November 1994: 47.

⁶⁹ George J. Stein, “Information Warfare” in *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds. (Fairfax: AFCEA International Press, 1996) 176.

⁷⁰ Please refer to the glossary in Appendix A for the full definitions.

⁷¹ John Arquilla and David Ronfeldt, *Cyberwar* 28.

Unlike traditional propaganda that seeks to provide information (true or false) which the adversary must understand, *netwar* or strategic information war attacks another society's epistemology and decision making process. Netwar attacks how the adversary knows, not just what the adversary knows.⁷²

The distinction between "what" and "how" adversary knows is not a trivial distinction, particularly if we are attempting to influence the decisions that an adversary must make.

Colonel Edward Mann, discussing Colonel John Boyd's OODA loop and orientation (the "how") argues:

Orientation gets nowhere near the attention from US military forces that observation does, yet it is probably the most critical element in the entire OODA loop. Colonel Boyd notes that "the second O, orientation—as the repository of our genetic heritage, cultural tradition, and previous experiences—is the most important part of the O-O-D-A loop since it shapes the way we observe, the way we decide, the way we act." In effect, orientation is the real starting point of the OODA loop, even affecting what we decide to observe (and then, what we decide to do). ...Orientation is the critical link between information—which is nice to have—and knowledge, which (when properly considered and acted upon) saves one from peril.⁷³

A case can also be made that propaganda, psychological operations, and deception have traditionally been associated only with military operations and, in general, targeted mass audiences with largely undifferentiated messages.⁷⁴ Additionally, the means for disseminating the messages were rather limited and unsophisticated, e.g. loudspeakers, leaflets, radio broadcasts, etc. Unsophisticated should not be construed as ineffective. On

⁷² Stein, "Information Attack" 7.

⁷³ Mann 4-14.

⁷⁴ Tactical deception operations are an obvious exception to this generalization.

the contrary, some of these means were quite effective under the proper circumstances.⁷⁵ According to proponents, the proliferation of information pathways and the increasing availability and effectiveness of technical media manipulation (e.g. morphing) have fundamentally altered the ability to conduct these operations. Messages can be tailored for individuals or small groups of decision-makers rather than mass audiences. The proliferation of computers, networks, fax machines, cellular telephones and satellite television provides multiple means, all vulnerable, to reach target audiences.

The psychological approach is not limited to technical means of manipulation; it can also include overt, public actions that have psychological impact. Included among the tools of this overt approach are concepts such as "public diplomacy" and "coercive diplomacy" According to Carnes Lord, public diplomacy encompasses three "distinct though closely related functions: international information, international political actions (or what may be called overt political warfare) and public affairs."⁷⁶ International information includes the functions performed by the United States Information Agency, particularly radio broadcasts. Lord notes that the inclusion of public affairs recognizes that it is impossible, in a modern democracy, to separate the information communicated to a domestic audience from that which is communicated to the international audience.

⁷⁵ Salvatore Sinatra, J., et. al. *Psychological Operations During Desert Shield/Storm* 2nd Ed. (MacDill AFB: USSOCOM, 1993) 5-3. An analysis of U.S. psychological operations conducted during the Gulf War credits these operations with affecting the surrender of 87,000 enemy prisoners of war. The primary means employed were leaflet drops, radio broadcasts, and loudspeaker transmissions.

⁷⁶ Carnes Lord, "The Psychological Dimension in National Strategy," *Psychological Operations: Principles and Case Studies*, Frank L. Goldstein, ed. (Maxwell AFB: Air University Press, 1996) 75-77.

The "public affairs" associated with public diplomacy differs from traditional efforts "by virtue of its strategic approach and its active effort to shape the domestic political agenda." Coercive diplomacy presupposes the use of military force to achieve political objectives.⁷⁷ Owens and Joseph Nye suggest that the United States' ability to "collect, process, act upon, and disseminate information" provides it with a significant advantage, an "information edge," in these efforts. This edge, properly employed, can serve as a force multiplier for diplomatic efforts.⁷⁸

Some writers, including Szafranski, have also posited the use of mind-altering chemicals or other stimulants as tools of IO:

The weapons of information warfare are not just those things affected by physical or material information systems...The weapons of the next generation could also include tools designed to enable entering and affecting the brain: sounds, smells, images, tastes, and feelings. They might include drugs. They might include pheromones.⁷⁹

Timothy L. Thomas also points out that the Russians are investigating approaches in psychotronics and psychotropics. They involve the possibility of manipulating people, either through psychological or physiological processes. Psychotronics involves the use of electrical pulses and sound waves to "induce hallucinations, sickness, mutations in human cells, 'zombification,' or even death." Psychotropics involve "medical preparations used to induce a trance, euphoria, or depression."⁸⁰ One product rumored to be the result of

⁷⁷ Lord 76.

⁷⁸ Joseph S Nye, Jr. and William A. Owens. "America's Information Edge" *Foreign Affairs* March April 1996: 20.

⁷⁹ Szafranski, "SIIOP," n.pag.

⁸⁰ Thomas, "Firewall," 89-90.

these efforts is the "Virus 666." Allegedly, this virus has killed more than 50 people by displaying a combination of number and color combinations on the computer screen that shuts down their bodily functions.⁸¹ Although there is little doubt that the Russians are actually conducting research, the existence of this type of weapon though is discounted and some claim that the "Virus 666" is an outright hoax.⁸²

Unlike the technological approach, which the DoD has publicly embraced, this particular psychological approach has not been officially declared a part of information operations. The closest military analog to these definitions is the DoD definition of perception management, which includes psychological operations but not propaganda:

Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.⁸³

The exclusion of propaganda is notable but not surprising given the negative connotations associated with it:

⁸¹ Timothy L Thomas, "The Age of The New Persuaders" *Military Review* May-June 1997: 78.

⁸² George Smith, "Truth is the First Casualty of Cyberwar." *Wall Street Journal* 8 September 1998: A28.

⁸³ DOD, *Joint Publication 1-02*, n.pag.

The U.S. public has historically identified propaganda and disinformation campaigns with communist and authoritarian regimes. Consequently, perception management is widely conceived as exemplary of the behavior that we struggle against in times of war, rather than a largely political tool whose moral character is *prima facie* neutral. Because American political culture equates democracy with unfettered public discourse, perception management is often regarded as anathema to our system of governance.⁸⁴

Many people seem to prefer the term “truth projection” to propaganda. This is, in many cases, attributable to a lack of understanding of propaganda. French author Jacques Ellul writes, “The most generally held concept of propaganda is that it is a series of *tall stories*, a tissue of lies, and that lies are necessary for effective propaganda.” Ellul stresses that propaganda must be truthful “in the realm of *facts*. The necessary falsehoods ...are in the realm of *intentions* and *interpretations*” (emphasis original).⁸⁵

Another word that is left out of all of the definitions cited, but implied nonetheless, is “manipulation.” This word and its connotations, like propaganda, are anathema to many people, particularly when government is involved. Thomas notes that it is usually associated with the propaganda of foreign governments despite the fact that it is very prevalent in our own society.⁸⁶ Yet, it seems that this is what is really at the heart of this approach to IO. If any serious attempts are made to utilize this as a strategic tool, it will require a considerable change in the strategic culture of the United States. In order to

⁸⁴ Rick Brennan and R. Evan Ellis. *Information Warfare in Multilateral Peace Operations --A Case Study of Somalia*. (Fairfax: SAIC, 18 April 1996). n.pag.

⁸⁵ Jacques Ellul, *Propaganda: The Formation of Men's Attitudes* (New York: Knopf, 1965) 52-53.

⁸⁶ Thomas, “New Persuaders,” 78

facilitate this change, the ethical and moral questions raised by this approach must be explored fully and satisfactorily answered.

Like the technological approach, the psychological approach has some shortcomings. The first and most significant is that human behavior is not always predictable; each individual responds differently to different stimuli. There is no guarantee that this approach will produce the desired result and the potential for unintended consequences is enormous.

Secondly, while many of the tools of this approach would be designed with deniability in mind, the political risks of compromise (both at home and abroad) are significant. These risks are magnified if the methods include, as Szafranski suggests, chemical substances. Some of the means contemplated under this approach (and the infrastructure approach) may conflict with established U.S. and international law or policy directives. Offensive IO is a particularly sensitive subject and is an unsettled and untested area of international law.⁸⁷

Third, the intelligence requirements of this approach are potentially immense. If tailored targeting of individuals is the goal, significant resources may be required to gather the information necessary to build a valid psychological profile. This also entails planners who are not merely familiar with psychology but knowledgeable or, preferably, expert. This skill is not readily available to most military planners. Additionally, the rapidly changing nature of communications technology places a burden on the

intelligence community to develop timely and detailed technical intelligence if the United States desires to exploit the vulnerabilities created by a dependence on technology. Vulnerabilities that exist today may disappear tomorrow. Conversely, new technologies may create new vulnerabilities. In either case, only detailed, up-to-date intelligence can identify the vulnerabilities.

Fourth, this approach requires a continuous, long-term strategy and detailed planning to be truly effective. If the goal is to prevent war or achieve our objectives without resorting to war, this approach should be applied before a crisis erupts. Of course, it may be applied during a crisis, but the efficacy of "crisis only" strategy would be doubtful. An individual's perceptions are the result of a lifelong accumulation of experience and the accompanying development of biases, both cognitive and motivated⁸⁸. Therefore, the manipulation of perception and epistemology must be a long-term process also; it is sheer hubris to believe that this can be done in short order, after a crisis has erupted. Indeed, if it was a simple matter, why not do it immediately and avoid crises altogether? Of course, it is not that simple and requires a consistent and well-conceived strategy, executed carefully and continuously.

⁸⁷ Lawrence T. Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo. *Information Warfare and International Law* (Carlisle Barracks: National Defense University Press, 1998) n.pag.

⁸⁸ Cognitive biases ("cool biases") are the result of interpreting evidence to fit existing preconceptions and theories. They result in seeing what we think we should see. Motivated biases ("hot biases") are the result of desires and emotions and affect decision-making. They result in seeing what we want to see.

Finally, a necessary corollary to the requirement for a long-term approach is the need for a joint and interagency approach. Since the DoD does not have the lead role in peacetime engagement, its activities must be coordinated with other agencies. Because this concept of IO is multidimensional and interdisciplinary, no single agency has all of the resources (particularly HUMINT) or expertise available to implement a truly comprehensive strategy of this nature. Close coordination is also essential to maximize the efficiency of any strategy and, more importantly, to avoid IO "fratricide," i.e. communicating conflicting information that nullifies another agency's efforts. This is no small task because of the bureaucratic politics involved. The struggle to achieve "jointness" within DoD has taken over a decade and there is still much progress to be made. Integrating the efforts of the DoD and a multitude of other federal agencies will require a great deal of effort. Again, these are not arguments against pursuing this approach but rather a call for a careful, unbiased evaluation of both the strategic goals and the means at our disposal for achieving them.

3. Other Views

There are several other approaches to IO which do not fit completely in the two classifications. Arquilla and Ronfeldt offer a similar, but more limited, concept, which they label "Cyberwar." Cyberwar is limited to the military arena but is conceptually broader than simple C2W. It appears to be a hybrid approach:

Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying, information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended.⁸⁹

Author Winn Schwartau also offers a somewhat different approach to IW. He defines information warfare as "an electronic conflict in which information is a strategic asset worthy of conquest or destruction. Computers and other communications and information systems become attractive first strike targets."⁹⁰ He also designates three classes of IW: Class I, Personal; Class II, Industrial and Economic Spying and Warfare; Class III, National, military or terrorist.⁹¹ While his definition has a technological slant, his classification of different types of IW precludes his from assignment to the two general categories that I have identified. In particular, the emphasis on and his approaches to personal privacy issues and corporate competition do not seem to fit well with concepts of strategic information operations (although there is some overlap).

The United States is not the only state grappling with the issues of IO and IW. Both China and Russia (as noted above) have also shown considerable interest in this

⁸⁹ John Arquilla and David Ronfeldt, *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: Rand, 1997) 30.

⁹⁰ Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, 2nd ed. (New York: Thunder's Mouth Press, 1995) 13.

⁹¹ Schwartau 17-20.

subject. On first reading, some of the literature would seem to be heavily influenced by or derived from American sources; it is difficult though to discern how much of Chinese and Russian thought on IO/IW has developed independently of American influence. Of course, it is also possible that some foreign writings have influenced American authors or that independent examinations have led to similar conclusions.

Some Chinese authors have adopted a technological approach similar to the one outlined in the previous section. The following definition of information warfare was presented by Liang Zhenxing to a conference held at the General Staff Research Institute of the People's Liberation Army:

All types of warfighting activities that involve exploitation, alteration, and paralysis of the enemy's information and information systems, as well as all those types of activities which involve protecting one's own information systems from exploitation, alteration and paralysis by the enemy.⁹²

It should also be noted that the Chinese viewpoint is not limited to this approach but, as a whole, reflects the same diversity found in American discourse on the subject. In the same paper, Zhenxing describes three types of information weapons that closely parallel some American concepts. The first consists of those weapons that "destroy the information infrastructure that the government, the armed forces, and important economic departments rely on for their effectiveness." The second includes "those weapons that use

⁹² Liang Zhenxing, "China: New Military Revolution, Information Warfare" Text from address translated by the Foreign Broadcast Information Service (FBIS). n.pag.12 Jan 1998.

procedures to induce powerful psychological reactions in personnel and control their actions.” The third type is “weapons that use wireless suppression procedures.”⁹³

Some Chinese authors have also adopted the view that digitizing the battlefield constitutes IW. In a paper excerpted from articles in the *Liberation Army Daily*, Senior Colonel Wang Baocun and Li Fei of the Chinese Academy of Military Science offer this definition of IW:

Information warfare is combat operations in a high-tech battlefield environment in which both sides use information technology means, equipment, or systems in a rivalry over the power to obtain, control, and use information. Information warfare is a combat aimed at seizing the battlefield initiative; with digitized units as its essential combat force; the seizure, control, and use of information as its main substance; all sorts of information weaponry [smart weapons] and systems as its major means.⁹⁴

Another Chinese author, Shen Weiguang, takes a very broad view of information warfare as a strategic asset:

...in the broadest sense, information warfare is a conflict in which a combat-ready military (as well as political, economic, cultural and technological) units employ force to occupy the infosphere and dispute each other's access to information resources. This refers chiefly to activities whereby a state employs information for the purpose of attaining strategic objectives.⁹⁵

⁹³ Zhenxing n.pag.

⁹⁴ Quoted in Michael Pillsbury, ed. *Chinese Views of Future Warfare* (Washington, D.C.: NDU Press, 1997) 328.

⁹⁵ Shen Weiguang, “Information Warfare – A New Challenge,” in *Infowar*, Gerfried Stocker and Christine Schopf, eds. (New York: Springer Wein/ ARS Electronica, 1998) 62-63.

Shen believes that IW encompasses six aspects: acquisition, application, protection, use, concealment, and administration of information. He also subscribes to the idea that "information warfare is without physical form or bloodshed."⁹⁶

While Russia has no official definition of IW, some unofficial statements reflect some of the same broad approaches found in American literature. Compare the following statements – the first by a Russian offered by a Russian Ministry of Defense civilian analyst:

Information warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation's decision-making system, on the nation's populous and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets.⁹⁷

Another Russian analyst offered another view, which indicates that the Russians appreciate the fact that IO is not limited to the battlefield:

⁹⁶ Weiguang 63.

⁹⁷ Thomas, "Russian Views," 27.

Both a broad and narrow sense are inherent in the existing concept of information warfare. In the broad sense, information warfare is one of the varieties of the "cold war"—countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, and so forth. ... In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them) and has as its goal the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this. The waging of information warfare in the narrow sense is the field of responsibility of mainly the ministers of defense of modern states.⁹⁸

In addition to the "psychotropic" methods mentioned earlier, the Russians are also pursuing a psychological approach based on the theory of "reflexive control," which is, at first glance, similar to the Szafranski/Stein approach outlined above. In reality, this approach is more concerned with conditioning the subject to respond than shaping perceptions. This approach seeks to capitalize on the motivated and cognitive biases of the audiences in order to achieve instinctive and habitual responses:

Reflexive control is a "branch of the theory of control related to influencing the decisions of others. In a military context, it can be viewed as a means for providing one military commander with the ability to indirectly maintain control over his opponent commander's decision process." Reflexive control involves creating a pattern or providing partial information that causes an enemy to react in a predetermined fashion without the enemy realizing that he is being manipulated. Its aim is to force an enemy commander to make a decision that, through the manipulation of information, was predetermined by the opposing side.⁹⁹

⁹⁸ Thomas, "Russian Views," 27.

⁹⁹ Thomas, "Russian Views," 27.

As a final note, it is interesting to note that skepticism about information operations is not limited by nationality. Thomas notes that some Russians, reflecting on the Strategic Defense Initiative (SDI) that was announced but never fully developed, believe that U.S. interest in IO/IW may be equally as bereft of substance. They view SDI as an exercise in reflexive control designed to bankrupt the Soviet Union and fear that U.S. IO/IW interests may be directed at achieving the same result with Russia.¹⁰⁰

4. Defensive Information Operations

Regardless of the approach to offensive IO, there is a consensus on the need to protect friendly information and information systems. Defensive information operations are commonly referred to as "information protect" or "information assurance." They are concerned with protecting the integrity and availability of friendly information and information systems. This can be accomplished through a variety of means such as providing physical security, maintaining operational security, and exposing adversary deception and propaganda. The two sides of the IO coin are obviously complementary; a thorough understanding of offensive measures should lead to a better appreciation of our own vulnerabilities and an understanding of how to defend against IO.

The President's Commission on Critical Infrastructure Protection recently issued a report that attempted to identify vulnerabilities in the national infrastructure and provided

¹⁰⁰ Timothy L. Thomas, "A Threat of Information Operations: A Russian Perspective." *War in the Information Age*, Pfaltzgraff, et. al. eds. (Washington, D. C.: Brassey's, 1996) 67.

recommendations on improving defenses against information attacks.¹⁰¹ A key problem in defensive IO however is attack assessment. Because the symptoms of many attacks may resemble ordinary system failures or user errors, it may be difficult to detect whether an IW attack is underway. Specific intelligence collection and analysis methodologies to assess the nature, extent and origin of the attack and predict likely enemy actions are required for defensive IO.

Much of the attention, mainly in the private sector, has been focused on the infrastructure protection and computer network security. There has been no significant public discussion of protection from propaganda, deception, and psychological operations. This may be a result of the democratic disdain for these types of operations. Additionally, the strategic culture of the United States views them as tactical or operational tools. It may also be that there is no way to prevent these operations; they can only be countered. It is obviously difficult in an open society to restrict access to any type of materials, particularly on the Internet.¹⁰²

While this aspect of IO is a necessary and important undertaking it will not be addressed in any detail. Because of their limited numbers, SOF are not well suited to defensive operations; they are primarily designed to carry out offensive operations. The

¹⁰¹ The President's Commission on Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructure* (Washington, D.C.: Government Printing Office, October 1997) Online. Internet. Available: www.pccip.gov

¹⁰² Frank L. Goldstein, ed. *Psychological Operations: Principals and Case Studies* (Maxwell AFB: Air University Press, 1996) 77-80.

exception is, of course, offensive tactical operations in support of a strategic defensive, which will be addressed in later chapters.

Table 2-2: Summary of IO Concepts

	Infrastructure and Information Systems	Psychological
Target Audience	Mass audience/entire population	Selected Individuals/leadership and decision-makers
Target.	Telecommunications, Electricity, Banking/Financial Services, Gas/Oil Production and Delivery, Transportation, Water Supply, Government and Emergency Services	Individual decision-making process via understanding (epistemology) and perception (biases).
Weapons	Computer Network Attack, (Viruses, Trojan Horses, Malicious Software, Trapdoors), Physical destruction	Psychological Operations, Deception, Propaganda,
Desired Effects	Cripple information dependent activities	Manipulate perception and understanding
Desired end-state	Capitulation - enemy is unable or unwilling to resist	Cooperation -decisions which support U.S. strategic objectives.

D. SUMMARY

The previous sections of this chapter have outlined the principal competing concepts of IO. Table 2-2 outlines the essential elements of each concept. The digitization of the battlefield and other attempts to strengthen our own C4I were excluded from the concepts because they are very traditional uses of information oriented towards the physical destruction of an adversary. The sections that followed described and contrasted the competing concepts of IO. The table below summarizes the main features of the two most prominent concepts.

III. THE STRATEGIC INTEGRATION OF SOF AND IO

Special Operations Forces have a dual heritage. They are the nation's penetration and strike force, able to respond to specialized contingencies across the conflict spectrum with stealth, speed, and precision. They are also warrior-diplomats capable of influencing, advising, training, and conducting operations with foreign forces, officials, and populations. One of these two generic SOF roles is at the heart of each ...special operations mission.¹

The previous chapter identified and discussed the principal concepts of IO. This chapter will examine the strategic integration of SOF and IO. First, the core competencies of SOF, those essential capabilities that separate SOF from other military forces, are examined. Second, the strategic utility of SOF, i.e. the contributions that these core competencies facilitate, is explored. Finally, the strategic integration of SOF and IO is examined in light of the core competencies and strategic utility of SOF.

At the strategic level, SOF will play a supporting role, as an instrument of statecraft, in an Information Strategy. The effective integration of SOF and IO should foster a synergy that enhances the strategic utility of both. It should also provide greater economy of force and more options than either IO or SOF can provide alone.

The strategic utility of SOF is directly related to their core competencies. Strategic utility is defined as "the contribution of a particular kind of military activity to the course and outcome of an entire conflict."² The core competencies in turn determine the nature of the contribution that SOF can make. These core competencies will also help determine what contribution SOF can make to the strategic application of the IO concepts developed

¹ DOD, *Annual Defense Report*, n.pag.

² Colin Gray, *Explorations in Strategy* (Westport: Greenwood Press, 1996) 163.

in the previous chapter. The core competencies of SOF identified in this chapter will also contribute to the analysis of future roles and missions for SOF in Chapter V. Understanding these core competencies is essential for maintaining the unique and “precarious value” of SOF during an era of change.³

A. SOF CORE COMPETENCIES

In organizational theory, core competencies are bodies of expertise, organizational skills, and systems, which are perceived as providing exceptional value and superior performance.⁴ They are not the same as the strategic utility, which reflects the ways that the core competencies are employed to influence the outcome of a particular conflict. They are substantially unique, and they typically lead the organization into new areas. A particular core competency may not be unique to the special operations community; it is the cumulative set of competencies that distinguishes this organization from its competitors.

The core competencies of the special operations community as a whole will be analyzed.⁵ This recognizes the fact that not every special operations organization (Special Forces, Seals, etc.) possesses identical skills but together they form a unique force

³ Susan Marquis, *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington, D.C.: Brookings Institution Press, 1997) 6-8.

⁴ C.K. Prahalad and Gary Hamel “The Core Competence in the Corporation.” *Harvard Business Review* May-June 1990: 79-91.

⁵ “Core competencies...cross SBU (strategic business unit) boundaries. They result from the interaction between different SBU competencies.” Mansour Javidan, “Core Competence: What Does it Mean in Practice?” *Long Range Planning* Vol. 31 (February 1998): 62.

package. It also recognizes that special operations are inherently joint operations.⁶ Three core competencies distinguish SOF from all other military forces. They are:

1. The ability to gain access to remote, denied, or politically sensitive areas.
2. Regional orientation.
3. Adaptability

Each of these competencies may exist, wholly or in part, in other defense organizations. However, this combination is unique and allows SOF to execute missions that other organizations cannot. These SOF skills are highly valuable in a dynamic and uncertain environment and contribute significantly to the increased demand for SOF.

1. Access

SOF have the ability to access remote, denied or politically sensitive regions of the world that conventional forces cannot access. The inaccessibility of a particular area may be due to political, logistical, or operational constraints. Regardless of the reason, the inaccessibility forces decision-makers to consider SOF. They offer “unique skills, tactics, and systems for the execution of unconventional, potentially high-payoff missions.”⁷ This is a primary reason that SOF offer “expanded options” – they give the decision-maker the option to reach the target in ways that other forces cannot. This ability is a highly valuable strategic asset.

⁶ Department of Defense, *Joint Publication 3-05. Doctrine for Joint Special Operations* (Washington, D.C.: Government Printing Office, 1998) I-2.

⁷ Dept. of Defense (The Joint Chiefs of Staff), *National Military Strategy: Shape, Respond, Prepare Now A Military Strategy for a New Era* (Washington, D.C.: 1997) n.pag. Online. Internet. Available: www.dtic.mil/jcs/nms/index.html

Obviously, if the mission is simply to destroy a target, precision guided munitions (e.g. Tomahawk missiles) can reach many targets around the globe this with less risk. In *The Future of War*, George and Meredith Friedman extol the virtues of precision munitions and predict the decline of many manned weapon systems.⁸ However, if the mission requires greater precision, deniability, or immediate battle damage assessment these munitions have limited utility. While the risk of collateral damage is substantially lower with PGMs, it is still a concern. Since very few nations possess this technology and the damage is substantial, their use is hardly deniable. Further, missiles have no utility if the mission requires the recovery of personnel or material. The recent strikes in Afghanistan and Sudan demonstrate both the utility and the limitations of this approach. While the missiles were able to reach the target area with no risk to U.S. personnel and caused substantial damage, they did not decapitate the terrorist organization of Osama bin Laden. Additionally, it took over a week for the U.S. to assess accurately the damage done by the missiles.⁹ SOF may have offered a more discreet targeting ability with immediate feedback, albeit at greater risk.

Similarly, unmanned aerial vehicles (UAVs) can accomplish many reconnaissance missions, although their range is more limited than missiles. Additionally, while UAVs

⁸ George Friedman and Meredith Friedman, *The Future of War: Power, Technology, and American World Dominance in the Twenty-First Century* (New York: St. Martin's Griffin, 1998).

⁹ While Osama bin Laden and his closest advisors were not publicly identified as the primary targets, one justification for the attack was the CIA belief that Bin Laden and his inner circle would be in the Afghan camp on August 20 (the day of the strike). Bruce Neelan, "Our Target Was Terror." *Time* Vol. 152 No. 9, August 31, 1998. n.pag. Online. Internet. Available: cgi.pathfinder.com/time/magazine/1998/int/980831/missile.html

may be able to loiter over an area for several hours, SOF have the ability to remain in an areas for days or weeks if necessary. SOF also have the ability to make immediate, intelligent appraisals of the situation and redirect their focus if necessary. They also have limited utility in densely populated urban areas, where targets can be easily masked from observation. While UAVs may be retasked in flight, current missiles cannot be retasked once launched. Additionally, both UAVs and PGMs are vulnerable to electronic countermeasures, particularly electromagnetic pulses. Like precision munitions, UAVs also reduce the risk to U.S. personnel.

Despite the shortcomings of PGMs and UAVs, Colonel Charles Dunlap argues that "technology may make it rarely necessary to risk elite troops on hazardous missions to conduct reconnaissance or sabotage." If required, he argues, conventional forces can accomplish deep strike missions.¹⁰ However useful, precision munitions and UAVs cannot establish a physical presence. Secondly, conventional forces lack the specialized training and equipment that allows SOF to accomplish this mission. Nor do they possess the language and cultural capabilities that allow SOF to train, advise, or equip foreign forces.

The issue of risk is not a trivial one; there are important domestic and international implications. Domestically, it is important to minimize the risk to U.S.

personnel, especially when the mission in question does not involve vital national interests. However, the amount of risk accepted can be a measure of commitment to a particular cause; both allies and adversaries are likely to draw inferences from a robust commitment, or lack thereof. If the United States is only willing to risk the cost of precision munitions, regardless of their effectiveness, this raises legitimate questions about significance of the commitment. The employment of SOF may provide a more convincing demonstration of commitment while at the same time reducing the associated risk to an acceptable level.

The ability of SOF to gain access is primarily a function of two key elements: specialized tactics, training, and equipment and a small force structure. The specialized tactics and training includes advanced infiltration and exfiltration techniques, communications capabilities, weapons employment, and medical skills. These skills allow SOF to access locations without revealing their presence when necessary. The special equipment used by SOF includes the transport platforms utilized by SOF (aircraft, ships, submersibles, etc.).

This small size of SOF operational units aids in maintaining low visibility in both permissive and non-permissive environments. This is particularly helpful in politically sensitive situations, particularly in the Middle East, where a large U.S. presence is

¹⁰ Dunlap suggests that Marine Expeditionary Forces (Special Operations Capable) can accomplish these missions. This reflects a poor understanding of the spectrum of capabilities of SOF and a questionable definition of what constitutes SOF. Charles J. Jr. Dunlap, "Organizational Change and The New Technologies of War." Paper presented to the Joint Services Conference on Professional Ethics (JSCOPE)

unacceptable to the host nation. SOF are trained and expected to be able to operate independently. Because of their small size and the short duration of most missions, SOF do not require extensive logistical support. The combination of small units and specialized training also allow SOF to operate without the extensive logistical support required for conventional forces. Additionally, the small size of SOF units allows rapid deployment to any location.

2. Regional Orientation

While SOF, as a whole, are capable of conducting operations on a global basis, components of SOF are regionally oriented with respect to language, culture and politics.¹¹ The language and cultural skills give SOF a true regional orientation unlike conventional forces, which focus on the climate and terrain of particular regions, not the people, and the culture. "It is because of the dual nature of global employment and regional orientation that SOF are well suited to operate in the post-Cold War world against adversaries threatening our national interests."¹²

The language and cultural skills of SOF represent a significant asset; they are well suited for a psychological approach to IO. They allow SOF to tailor their messages to

Washington, D.C. Jan 30, 1998. Online. Internet. Available: www.usafa.af.mil/jscope/Dunlap98.HTM

¹¹ The exception to this is the aviation component (AFSOC and TF-160) and Army Rangers. While the aviation elements are regionally oriented with regard to mission requirements, they do not typically have any language or cultural requirements. The Ranger battalions are primarily a direct action force used to facilitate forced entry.

¹² Blackburn, et. al., *A National Policy For Deterring The Use Of Weapons Of Mass Destruction*. Research Paper, Air Command and Staff College, Maxwell AFB, April 1996: 22.

local audiences and assist others in developing psychological operations and perception management campaigns. They also allow SOF to gain the confidence of local audiences. In addition to merely possessing the ability to communicate in another language, SOF are also culturally and politically aware. Coupled with the small size of SOF units, this capability makes SOF ideally suited to forward deployments in politically sensitive areas; SOF can conduct operations without the political risks associated with larger conventional forces.¹³ SOF can also help project a positive image of the United States; humanitarian assistance and civil affairs projects can help shape the perceptions of the host nation population and government. While foreign troops are certain to engender some resistance, people generally look upon foreign soldiers who speak their language and respect their customs more favorably. Additionally, the experience and maturity of SOF operators usually precludes the types of incidents that would anger host-nation citizens.

Another asset is the institutional knowledge of foreign forces and governments, gained first-hand through habitual association including military-to-military contacts and noncombatant missions like humanitarian assistance, security assistance, and peacekeeping. Because of their regional orientation, SOF operators are frequently assigned to the same unit for extended periods. This affords them the opportunity to deploy repeatedly to the same areas and often work with the same forces. It also allows them to develop and maintain an intimate knowledge of specific areas of operation. This is *sui generis* within the armed forces.

¹³ DOD, *Joint Pub 3-05* vii.

3. Adaptability

SOF have repeatedly demonstrated an ability to apply their skills to a variety of tasks (e.g. humanitarian demining) and deal with complex issues (e.g. implementation of the Dayton Accords in Bosnia). This core competency is another reason that SOF offers expanded choices for decision-makers. This adaptability is the result of several factors: willingness to innovative and try unconventional approaches; organizational flexibility; and the maturity of SOF personnel.

According to Colin Gray, special operations can provide a laboratory for innovation. The small scale and high risk of special operations requires that SOF adopt “‘equalizing’ techniques and equipment.”¹⁴ The unique organizational culture of SOF also contributes to innovation. Although USSOCOM is only a decade old, the history of US special operations is obviously much older and USSOCOM has inherited the heritage of U.S. special operations. While the heritage of each service component is unique, they all embody similar qualities: extraordinary courage, self-reliance, and dedication to excellence. All of these qualities lead to a “can-do” attitude, which fosters a willingness to innovate in order to accomplish the mission.

SOF employ small units and a flexible command structure that can be easily adapted to a variety of situations.¹⁵ A Joint Special Operations Task Force (JSOTF) can be established and tailored to meet the needs of a particular mission. At the strategic

¹⁴ Gray 175.

¹⁵ There is no comparison to other “small units,” e.g. an infantry platoon; it is not an operational unit and has no ability to sustain itself.

level, the tasks assigned to SOF are centrally planned but operational and tactical execution is decentralized; most operational details are determined by the operators themselves. "Delegation of execution authority to responsible and capable lower-level commanders is essential to achieve effective span of control and to foster initiative, situational responsiveness, and tactical flexibility."¹⁶ The rapid deployability of SOF also enhances flexibility by allowing forces to be concentrated or dispersed on short notice.

The maturity and experience of SOF personnel contributes to adaptability. Since SOF personnel are frequently older and more experienced than other forces, they are better able to deal with complex missions. Nearly all SOF organizations conduct a rigorous assessment and selection to find the candidates with the highest potential for success in special operations. Further, all SOF also undergo realistic and stressful training not only during their initial training but also in their units. Because of their small size and global commitments, SOF are more likely to execute assigned missions with little or no direct supervision. Their maturity and experience offer some assurance to decision-makers that they have the necessary skills to accomplish a mission.

B. THE STRATEGIC UTILITY OF SPECIAL OPERATIONS

Special operations (SO) differ from traditional military operations in several important aspects. First, SO are generally small-scale operations because most large forces do not possess the skills, strategic mobility, or low visibility of SOF.¹⁷ Second, SO

¹⁶ Department of the Air Force, *AFDD 1: Air Force Basic Doctrine* (Washington, D.C.: Department of the Air Force, 1997) 23.

¹⁷ Gray 145-146.

involve a high degree risk, both physical and political. Special operations "are characterized by a narrow window of opportunity, low requirement for repetition, and a high consequence of failure."¹⁸ This is particularly true when they are conducted in remote or denied areas with little friendly support.. They also can involve a high degree of political risk; failure can damage national prestige. Third, although SO often employ unconventional tactics and weapons, it is usually the missions themselves that are unorthodox.¹⁹ Gray also adds that SO may be clandestine, covert, or overt and that they seek to achieve "significant political or military objectives" in support of foreign policy.²⁰

For Colin Gray, "[s]pecial operations are an agile, real-time, intelligent, and discriminating instrument of grand and military strategy."²¹ Like any other force or military capability, the strategic utility of SOF is dependent upon the context in which they are utilized. Gray reminds his readers that the strategic utility of SOF "depends at least as much on the imagination and the competence of their political masters as it does on their tactical effectiveness."²² SOF can achieve strategic effects both directly, i.e. through the immediate consequences of their actions, and indirectly, i.e. through the operations which they make possible.

¹⁸ James A Cerniglia, et. al., "The DIM MAK response of Special Operations Forces to the World of 2025: "Zero Tolerance/Zero Error," *Air Force 2025*, Vol. 3, Ch. 11. (Maxwell AFB: Air University. August 1996) vi.

¹⁹ Gray 146.

²⁰ Gray 147-149.

²¹ Ibid.173.

²² Ibid.149.

Gray identifies two broad categories of “master claims” on the strategic utility of SOF: economy of force and expansion of choice. To these, USSOCOM adds a third: “tailor-to task capabilities.”²³ These claims of utility relate mainly to the direct results of SO involving the use of force or requiring access to denied or hostile environments. Gray also identifies seven “other claims” on the strategic utility of special operations: innovation, morale, showcasing of competence, reassurance, humiliation of the enemy, control of escalation, and shaping the future.²⁴ With the exception of innovation, these claims of utility relate mainly to the psychological effects generated by special operations.

1. Economy of Force

Because of their small size and special skills “special operations can achieve significant results with limited forces.”²⁵ The financial cost and scale of effort necessary to support special operations is considerably lower than that required for conventional forces. These results may be achieved through either the unilateral employment of SOF or integrated operations with conventional forces.

While SOF are “uniquely suitable for execution of *coups de mains*” they are also able to execute missions that enhance the effectiveness of regular forces. This can be accomplished in several ways. First, technological advances put potent, precision weapons in the hands of small forces or individuals. SOF possess the skills necessary to

²³ United States Special Operations Command (USSOCOM), *United States Special Operations Forces: Posture Statement 1998* (Washington, D.C: Government Printing Office) 7.

²⁴ Gray 168-180.

²⁵ Ibid. 168.

attack and disable strategic targets; they are uniquely qualified to gain access to critical targets and employ these weapons. The ability to gain access to high value targets also allows SOF to provide terminal guidance for standoff munitions. Both methods provide a means to reduce or degrade an aggressor's ability to threaten U.S. interests or reduce the requirement for large conventional forces. Special operations in an enemy's rear area may distract or deceive the enemy and cause him to divert combat power from the main battle area.²⁶

Secondly, the ability of SOF to train and advise foreign forces can directly reduce the need for U.S. forces by enhancing the utility of indigenous forces. Third, the small size, rapid deployability, and independence of SOF also means that they can be deployed to multiple locations more quickly than conventional forces to provide a U.S. presence. This may provide a deterrent effect until conventional forces can reach the area or thwart an adversary's attempt to gain a political or military advantage.

2. Expansion of Choice

Gray points out that "policy without means is just wishful thinking."²⁷ SOF provides the means to accomplish missions that other forces cannot and thereby provide decision-makers with expanded options. They expand national capabilities to react to situations requiring regional orientation and cultural and political sensitivity. This is particularly true in peacetime, when political considerations and constraints on the use of force may be higher than during war. SOF can apply military and political pressure

²⁶ Gray 172-173.

discreetly “when no other class of military action is politically feasible.”²⁸ SOF provide the ability “to influence certain events with forces that are smaller and less visible than conventional formations, offering the NCA options that do not entail a major military commitment.”²⁹ It must also be noted that SOF can accomplish many of their assigned missions without the use of force. During crises and contingency operations, SOF offer a range of options that “fall between wholly diplomatic initiatives and the overt use of conventional forces.”³⁰

During wartime, because SOF can reach areas or targets that conventional forces cannot, they allow commanders to “assign missions which offset the limitations of regular forces.”³¹ In doing so, SOF may “entice the enemy into an overextension of forces.”³² This may create vulnerabilities that can be exploited by conventional forces or even other SOF. The bottom line on SOF missions is that “special operations forces are selected, equipped and trained to do what regular forces cannot do” and therefore expands the choices available to decision-makers.³³

²⁷ Ibid. 174.

²⁸ Ibid. 173.

²⁹ Dept. of Defense (The Joint Chiefs of Staff), *National Military Strategy: Shape, Respond, Prepare Now A Military Strategy for a New Era* (Washington D.C., 1997) n.pag. Online. Internet. Available: www.dtic.mil/jcs/nms/index.html

³⁰ USSOCOM, *1998 Posture Statement* 7.

³¹ Gray 172.

³² Ibid. 173.

³³ Ibid. 149.

3. Tailor-to-Task Capabilities

This is the result of the core competence of adaptability. This quality allows SOF to adapt to a wide and constantly varying range of tasks and conditions. The numerous skills resident in SOF and the experience and maturity of SOF operators allow them to be used in a variety of situations. Whether a mission involves penetration of a denied area or providing humanitarian assistance, SOF can be quickly and efficiently task organized to accomplish the mission.³⁴

4. Other Uses

Of the seven "other claims" that Gray identifies, six relate to influencing political will and commitment. Gray notes that "one can design special operations of a military or political-psychological nature for the purpose of securing strategic effect on the political level of conflict."³⁵

Two of these other claims, raising morale and offering reassurance, are related to mainly to the domestic audience. Special operations can raise the morale of the public, other military forces, and allies and therefore "encourage a sustained political will."³⁶ They can also provide reassurance to an uneasy public (or ally) that "something is being done" about a problem. The Son Tay raid provides a good example of both of these dynamics in action. Although the raiders were unsuccessful in bringing home any POWs, the raid itself raised morale, especially among prisoners; it demonstrated to the public, the

³⁴ USSOCOM, *1998 Posture Statement* 7.

³⁵ Gray 180.

³⁶ Ibid. 175.

military, and the prisoners that the U.S. was acting aggressively to recover captured servicemen.³⁷

The claims of "showcasing competence" and "humiliating the enemy" are related mainly to the international audience and are corollaries to the morale and reassurance claims. A display of competence can also serve to reassure a domestic audience and humiliating an enemy can raise morale on the home front. The use of SOF for either purpose can enhance deterrence. "Military competence is a prerequisite for deterrent effect" and recognition of this competence enhances deterrence. The exemplary use of SOF not only demonstrates this competence but can damage an adversary's reputation by dealing him an embarrassing blow.³⁸ Again, the Son Tay raid demonstrated the competence of U.S. SOF and may have embarrassed the North Vietnamese. At the very least, it highlighted their vulnerability and caused them to alter their behavior with respect to POWs.³⁹

When properly employed, the well-deserved reputation for tactical excellence enjoyed by U.S. SOF may at least delay, if not deter, aggressors who are unsure about

³⁷ The desire to reassure the prisoners was an explicit consideration for Secretary of Defense Melvin Laird. He later recalled that "one of the things that convinced me more than anything else to recommend...that this operation go forward was my discussions with several of the prisoners who were released [by Hanoi earlier]...I heard their concern that we in the United States had forgotten them. In order to maintain oneself for 5,4,3 years, there must be hope, and according to these men many of our prisoners were losing their hope and faith. I felt that this was important to their survival." The morale of the prisoners improved significantly, as did their treatment. Quoted in Lucien S Vandenbroucke, *Perilous Options: Special Operations as an Instrument of U.S. Policy* (New York: Oxford University Press, 1993) 64.

³⁸ Gray 178.

U.S. commitment. The deployment of U.S. SOF to a region can send a strong signal to would-be aggressors about U.S. commitments. Indeed, "if special operations forces have a reputation for effectiveness, their use – even just the announcement of their commitment – can have a deterring effect."⁴⁰

The other claims related to influencing political will and commitment are "controlling escalation" and "shaping the future." The employment of SOF instead of conventional forces can offer a means to "limit the scope and intensity of a conflict."⁴¹ Using SOF for this purpose is contingent upon not humiliating the enemy. The operation must walk a fine line between inflicting enough a damage to coerce the enemy and inflicting so much damage that the enemy feels the need to retaliate. It is in this situation that the ability of SOF to engage targets precisely, without causing collateral damage, is very beneficial. The small scale and precision of special operations may allow them to inflict damage discreetly without forcing an adversary to escalate. According to Gray, "It is much easier for a foe to choose to ignore small-scale operations than large-scale operations."⁴² Gray's hypothesis here is that there will not be as much public or political pressure for retaliation if the operation is limited in scope and in terms of damage inflicted.

Special operations may be used to shape the future in several ways. One possible means is by causing the enemy or adversary to expend resources in response to a

³⁹ Vandenbroucke 69.

⁴⁰ Gray 176.

⁴¹ Ibid. 178.

perceived threat. This expenditure may limit the adversary's future options and thereby "shape the future." Gray notes that it may be difficult to design operations to achieve this effect and that it is more often by accident that such effect is generated.⁴³

Special operations can also help to shape the future of course of events by promoting stability and thwarting aggression. They can provide security assistance and training to struggling or nascent governments to help ensure their survival. Their presence can also shape favorably the views of local populations towards both the U.S. and the host nation government. They can also provide "a tangible and impressive gesture of political interest" that may dissuade potential aggressors.⁴⁴

The last claim of strategic utility is innovation. Eliot Cohen refers to this as the "laboratory role."⁴⁵ Gray notes that "special operations can demonstrate new tactical doctrine, equipment, and military methods." He notes that this is often a necessitated by the nature of special operations. This innovation can also benefit conventional forces that frequently adopt equipment and methods developed by SOF.⁴⁶

5. The Misuse of SOF

No discussion of the strategic utility of SO would be complete without a word on the potential misuses and drawbacks in the employment of SOF. While SOF provide

⁴² Gray 179.

⁴³ Ibid. 173.

⁴⁴ Ibid. 180.

⁴⁵ Eliot A. Cohen, *Commandos and Politicians: Elite Units in Modern Democracies*. (Cambridge: Harvard Center for International Affairs, 1978) 31-32.

⁴⁶ Gray 174-175.

some strategic benefits, they are not a panacea or silver bullet for every political or military dilemma. Neither are they a substitute for competent conventional forces. Understanding this last point is critically important, in light of the large reductions in conventional forces and increasing commitments, decision-makers may be tempted to look to SOF when a conventional force would be better suited to the task.

Egregious misuse can result from wishful thinking on the part of political leaders coupled with a failure by military leaders to emphasize the limitations of SOF.⁴⁷ Eliot Cohen attributes some cases of misuse to the “romantic politician” who is enamored of the heroic image of “elite units.”⁴⁸ According to Lucien S. Vandenbroucke:

Decision makers can become insidiously attracted to strategic operations, to the point of engaging in wishful thinking, in which hopes distort perception and wishes are mistaken for reality.⁴⁹

This combination can have disastrous political and military effects. Gray notes that if “special operations can enhance political respect, it is likewise true that failure can diminish national standing.”⁵⁰

The Iranian hostage rescue attempt (Operation Eagle Claw) is a clear example of this type of misuse and the disastrous military and political results. Hamilton Jordan, the White House Chief of Staff under President Carter wrote in his memoirs that he was “excited by the prospect of a bold and successful resolution of the crisis,” so much so that

⁴⁷ Gray 183.

⁴⁸ Cohen 35-44.

⁴⁹ Vandenbroucke 7.

⁵⁰ Gray 181.

he “couldn’t even contemplate failure.”⁵¹ Secretary of State Cyrus Vance strenuously objected to the plan but met with “awkward silence.”⁵² The senior officers most closely involved in planning the operation also failed to explain adequately to the political leadership the risks of this operation.⁵³

The political implications and sensitive nature of many special operations can also encourage excessive control by political leaders.⁵⁴ This temptation may increase as improved communications make it possible to direct operations anywhere on the globe. The small size of SOF units may also present a more inviting target for micro-management than larger conventional forces.

The employment of SOF may also have unintended consequences. For example, an enemy humiliated as the result of a special operation may actually escalate a confrontation. Similarly, he may emerge with a strengthened resolve to continue to fight. Tactical failure also threatens serious consequences; it can reduce available forces and create a capability gap that cannot be bridged quickly. By their nature, SOF are few in number and difficult to replace quickly. Additionally, the use of SOF may be a “wasting asset,” i.e. an adversary can take precautions once he is aware of a specific capability.

⁵¹ Vandenbroucke 143.

⁵² Ibid. 139.

⁵³ Ibid. 135.

⁵⁴ Ibid. 7.

Special operations may also alert an adversary to impending conventional operations or lead to an overall increase in security.⁵⁵

C. INTEGRATING SOF AND IO

Given the competencies of SOF and the strategic utility of SO, how can SOF support IO? The role of SOF in an IO campaign may differ based on the objectives of the campaign but the capabilities of SOF have utility for both the psychological and infrastructure approaches. Depending on the circumstances, each specific, tactical SOF mission may support a larger strategic information operation.

1. Supporting the Psychological Approach

According to Alan Campen, "It may not be too much to say that every single activity for SOF will be an act of information operations."⁵⁶ While this may be hyperbole, Gray makes a similar observation that any special operation can be designed to have psychological effects. Because SO are applicable to the entire spectrum of conflict, the ability to achieve psychological effects is also applicable across the entire spectrum. The effect generated by each mission will be dependent upon not only the type of mission but also the circumstances surrounding it. This means that there are myriad possibilities for generating psychological influence. While there are too many possibilities to address each specifically, it is possible to generalize.

⁵⁵ Gray 181.

⁵⁶ Campen, Alan C. From personal correspondence (e-mail) with the author. 2 Nov 98.

The most frequent image of SOF is that of a Navy SEAL or Army Special Forces soldier; few people think of the psychological operations soldier as part of SOF. Yet, the value of the psychological operations units cannot be overlooked. They provide the most direct means of integrating SOF and a psychological approach to IO. They also provide a capability that is not available from other forces in any way, shape, or form. This is especially true of the EC-130E Commando Solo aircraft; which offers a variety of broadcast, reception, and analysis capabilities. Psychological operations forces, trained in the methods of persuasion and, like other SOF, regionally oriented, can provide direct support to an IO campaign across the spectrum. An important role for psychological operations forces is amplifying the messages conveyed by the actions of other SOF and other U.S. forces.

Civil Affairs units also play an important role in fostering favorable images of the United States. Their skills can help to promote stability and provide reassurance to domestic and foreign audiences. Their skills are particularly valuable in the wake of conflict or natural disasters. By helping to establish or restore an effective civil infrastructure they can also help shape the future.

Other SOF forces also have a role in supporting the psychological approach to IO. During peacetime, the majority of special operations conducted do not involve the use of force or penetration of denied areas (e.g. DA, SR, UW), for both practical and political reasons. The missions most likely to generate a psychological effect in peacetime are the missions that involve supporting or assisting our allies (e.g. FID, CA, HA, HD, PO, SA). These operations can be extremely useful for generating a positive image of the United

States; they can create lasting impressions and incline the host-nation population to support the strategic goals of the United States. The effects generated by these operations will support claims of shaping the future and providing reassurance.

The exceptions may be counter-proliferation and combating terrorism but these missions are conducted rarely, at least with public knowledge. SOF can provide "the tools to disarm an adversary unilaterally if necessary, before the adversary can initiate the use of WMD." The fact that the public is unaware of these activities limits the scope of psychological effect. Nonetheless, a successful special operation against WMD proliferators may achieve a deterrent effect by displaying competence, even if the audience is limited. For instance, a successful SOF strike against a well-guarded and concealed facility used to produce WMD may generate psychological effects not only on the actual target but also on other states that possess these types of facilities.

In order to achieve the maximum deterrent effect from a single low-visibility operation the U.S. may need to "advertise" its success to other potential targets discretely. This "advertisement" would itself be a type of information operation designed to influence other proliferators. "Preemption can in itself have a deterrent effect by threatening the adversary with further destruction if it attempts to use any remaining WMD or to rebuild its arsenal. Additionally, preemption may make a significant impression on other proliferant actors, thus deterring them from WMD use."⁵⁷ If these special operation actions deter other actors from pursuing WMD, this would also support a claim of shaping the future.

An intriguing variation on this theme involves the possibility of advertising a capability that does not actually exist or is not fully developed. This type of strategic deception can have profound effects on an adversary's behavior. Although it involved ballistic missile defense rather than SOF, the Strategic Defense Initiative (SDI) is useful for examining the possible consequences of advertising a notional capability. The exemplary use of a capability may force our adversaries to take measures that they can ill afford financially. Even if the costs are significant, an adversary may be willing to bear them in order to protect his vital strategic capabilities. This expenditure may undermine the adversary's ability to achieve other strategic goals.

Despite the lack of a demonstrated capability, many people believe SDI contributed significantly to the collapse of the Soviet Union by prompting exorbitant expenditures to cope with a perceived threat. Former Soviet diplomat Andrei Gromyko charged that "behind all this lies the clear calculation that the USSR will exhaust its material resources and therefore will be forced to surrender."⁵⁸ According to Margaret Thatcher, "The final straw for the Evil Empire was the Strategic Defense Initiative."⁵⁹ Regardless of whether this assessment is correct, it remains true that a notional capability, properly "advertised," can exert significant pressure on adversaries.

⁵⁷ Blackburn et. al. 20-21.

⁵⁸ Quoted in Dinesh D'Souza, "How Reagan Won the Cold War." *National Review* 24 Nov 24 1997: 36-41.

⁵⁹ Margaret Thatcher, Speech. The Heritage Foundation 's 25th Anniversary, Washington, D.C., December 10, 1997. n.pag. Online. ProQuest Direct.

Certainly, there are risks involved with advertising a capability, real or notional. In both cases, the exemplary use of SOF may generate a response that diminishes or eliminates the potential for successful SO in the future. This is particularly true if low-cost counter measures are available. Additionally, it may encourage actual strategic or tactical innovation that poses a real threat to the security of the United States.

While SOF can generate psychological effects in peacetime without the use of force, the situation is generally reversed during wartime. Combat-type missions increase in frequency and importance, generating a greater psychological effect on the enemy while the other non-combat missions become less frequent, depending on the scale of conflict. The effects generated by these operations will support claims of showcasing competence and humiliating the enemy. They may also support the claims of shaping the future and controlling escalation. The collateral activity of combat search and rescue is an important means of offering reassurance and boosting morale.

An additional means for SOF to provide support for strategic IO oriented on psychological influence is through the collection of intelligence on the attitudes, perceptions, and beliefs of foreign audiences. The language and cultural abilities of SOF coupled with habitual association put them in a unique position to gather this type of intelligence. Another way for SOF to support IO by providing intelligence is through the coalition support mission. This allows SOF to provide accurate intelligence on the activities and disposition of coalition forces, which may be important to a strategic IO campaign. SOF can also play a role in the psychological approach by uncovering enemy deception. The unique abilities of SOF to gain access to denied areas may allow them to

either corroborate or deny other sources of intelligence on enemy activities, capabilities, and intentions.

2. Supporting the Infrastructure Approach

SOF can provide an enhanced offensive capability to the infrastructure approach. The ability of SOF to gain access to remote or denied areas allows them to gain access to isolated or well-protected computer networks, important telecommunications nodes, or other information systems. SOF provides the ability to attack high value infrastructure targets. Attack does not necessarily imply physical destruction of these targets; it can include discretely disabling them using EMP, HERF, or HPM weapons.⁶⁰ These weapons currently have limited ranges and therefore require the operator to be in close proximity to the target. The capability of SOF to gain this access makes them ideally suited for this type of weapons system; they can infiltrate the enemy's rear area and employ these weapons near critical targets. Because of the directional capabilities of this weapon, it can target specific devices, possibly confusing any attempt to troubleshoot the perceived problem. The directional nature may also provide precision targeting of systems shared by civilian and military targets to avoid collateral damage. Additionally, these weapons offer a measure of deniability not possible with conventional munitions. "Precision-neutralization operations conducted against high-value targets require extreme precision, timing, coordination, and offer the added value of deniability."⁶¹

⁶⁰ It is important to recall that these weapons are still in development.

⁶¹ Cerniglia, et. al. 8.

“Attack” may also imply gaining access to enable other information operations. For example, SOF may provide an ability to tap into fiber optic cables in order to monitor or the data flowing through those lines. The ability to gain access also allows SOF to collect intelligence on adversary information systems. This may include the use of special monitoring equipment that requires close proximity to the targeted information system. This may be a critical role for SOF since battle damage assessment of attacks on information systems may be difficult.

Some of the collateral activities conducted by SOF have a limited utility for the infrastructure approach. The utility is limited to gathering information about infrastructures. This is a sensitive issue, especially when conducting peace operations or humanitarian assistance.

3. Supporting Defensive IO

The previous chapter briefly discussed defensive IO and noted that the role of SOF would be limited. While defending against adversary IO is a necessary and important undertaking, it is not a function well suited to SOF. Special operations forces are, by nature, offensively oriented and would play a small role in defensive information operations. Actions taken to defend against adversary IO primarily consist of passive measures; i.e. they do not require any direct action against potential adversaries. Because of the passive nature of this activity, most organizations will have the same primary responsibilities: maintaining operational security; providing physical protection for their own information systems; and ensuring the security of information systems through the use of appropriate computer security measures. Therefore, in conducting defensive

information operations, the role of SOF will be essentially similar to other military and governmental organizations.

The nature of defensive IO is another factor that will limit the participation of SOF. Defensive IO during peacetime is primarily a domestic enterprise and the domestic use of all military forces is severely restricted.⁶² Other federal agencies, like the FBI, and DoD agencies, like the National Security Agency (NSA) and the Defense Information Services Agency (DISA), are better equipped and specifically charged with performing most defensive IO functions.

One possible exception is the use of SOF as a means to seize "hackers," programmers, or other personnel responsible for conducting or facilitating infrastructure attacks on U.S. systems. These operations may be conducted to pre-empt planned attacks or in response to actual attacks. Because small groups or individuals can carry out these attacks and because they may not cause significant physical destruction, responding with conventional forces may be impractical. However, SOF are capable of precision targeting to destroy the adversaries capability and they are capable of recovering the personnel involved in the attacks. This role for SOF would likely resemble their role in responding to terrorist incidents.

⁶² As a general rule under the Posse Comitatus Act (Article 18 of the U.S. Code 1385), Department of Defense personnel and equipment may not be used in a domestic law enforcement capacity. However, in 1981, Congress enacted an exception that authorized specific Department of Defense assistance in drug interdiction and drug eradication operations (Article 10, U.S. Code 371-380).

Because of the low entry costs and high availability of the tools necessary to conduct infrastructure attacks, it is unreasonable to believe that an adversary can be prevented from *acquiring* a capability. However, it may be possible to prevent him from *employing* this capability through pre-emptive strikes. Of course, this type of action brings considerable political risk but SOF is well suited for this. SOF offers a degree of deniability that is not available with conventional weapons or forces. The mobility of SOF may also be an asset in catching up to mobile hackers who are not tied to any particular geographic location. This could be an information-age version of the Gulf War SCUD hunt. It may also prove to be equally as difficult without detailed intelligence and close coordination with computer emergency response teams (CERT). Much like sizing drug dealers, terrorists, and other international criminals, this type of operation has a variety of legal implications. For example, do attacks against computer networks constitute a crime under international law? If so, does the United States have the authority to seize the perpetrators? The situation may become even more complicated if the perpetrator is an employee of a foreign government.

As noted in Chapter II, defending against adversary IO includes more than protecting infrastructure. From the psychological perspective, it means countering attempts to manipulate perceptions, understanding, or and opinion. In this regard, SOF offer the same support to defensive IO that they offer to offensive IO. Another potential defensive use of SOF involves DA and SR missions to provide undeniable evidence to counter the claims of an adversary. This type of effort may be extremely useful in counter-proliferation efforts where a state denies that it possesses WMD or is attempting

to develop WMD. Like all operations that involve a violation of territorial integrity in the absence of armed conflict, this may present significant political risk. Because of the risk involved, the quality and authenticity of any evidence recovered must be irrefutable.

D. ADVANTAGES OF INTEGRATION

Using SOF to conduct or support IO provides the same benefits to IO as it does to other missions. SOF provide economy of force, expansion of choice, and tailor-to-task capabilities for decision makers considering IO. Economy of force is achieved not merely because of their small numbers but because of the disproportionate effects that SOF can produce. This is particularly true for supporting the psychological approach. A single SOF strike deep in enemy territory against can generate psychological effects that are disproportionate to the physical threat that SOF present.

Because SOF skills are applicable across the entire spectrum of conflict, they provide options for situations where conventional forces are not appropriate. For infrastructure IO, the ability of SOF to gain access to remote targets expands the scope of available targets. This provides decision-makers with alternatives to the use of conventional forces or precision guided munitions. For the psychological approach, the language and cultural skills of SOF provide a means to directly influence target populations that would not otherwise be available.

Finally, SOF can provide a degree of deniability not available with conventional forces or precision munitions. This applies to support for both approaches to IO. because they have a small footprint and can maintain a low profile, SOF may be employed under circumstances that preclude the use of conventional forces, either for political or

economic reasons. "SOF provide both a "transparent" presence as well as the operational "punch" to accomplish many extremely dangerous, politically sensitive, and highly technical missions."⁶³

E. SUMMARY

This chapter identified three core competencies of SOF: access, regional orientation, and adaptability. SOF offers strategic utility as a result of employing these competencies. These core competencies allow SOF to provide economy of force and expanded choices for strategic decision-makers. Additionally, the employment of SOF can influence the political will and commitment of both allies and adversaries. The core competencies of SOF provide unique skills that are well suited to conducting or enhancing IO. The ability to gain access to remote or denied areas is highly useful for the infrastructure approach to IO. It provides the ability to reach targets that other IO means cannot while at the same time providing an economy of force. The regional orientation and adaptability of SOF enhance this capability. As the field of IO matures, SOF are well suited for developing and implementing innovative approaches. SOF also a variety of options for supporting the psychological approach to IO. Whether they are conducting deep strike, counter terrorist, or humanitarian assistance operations, the employment of SOF can generate a strategic psychological effect. Again, because SOF provide economy

⁶³ Blackburn, Dale A., et. al. *A National Policy For Deterring The Use Of Weapons Of Mass Destruction*. Research Paper, Air Command and Staff College, April 1996. Online. Internet. Available: www.au.af.mil/au/database/research/ay1996/acsc/96-102.htm

of force and expanded choices they increase the scope of operations available to influence friend and foe.

The tables below summarize the utility of SOF for each approach to IO under different levels of conflict. While the categories of peace, conflict, and war have become somewhat blurred in the information age it is still necessary to somehow delineate the intensity and scope of conflict. The tables indicate that SOF offers more support to the psychological concept of IO than to the infrastructure concept. However, the SOF skills involved in direct action and special reconnaissance offer robust support to the infrastructure approach. It is also interesting to note that the collateral activities offer no real support to the infrastructure approach.

Table 3-1: IO Utility of Principal SOF Missions

MISSION / ENVIRONMENT	INFRASTRUCTURE			PSYCHOLOGICAL		
	PEACE	CONFLICT	WAR	PEACE	CONFLICT	WAR
DIRECT ACTION						
SPECIAL RECONNAISSANCE						
FOREIGN INTERNAL DEFENSE						
UNCONVENTIONAL WARFARE						
COMBATTING TERRORISM						
COUNTER PROLIFERATION						
PSYCHOLOGICAL OPERATIONS						
CIVIL AFFAIRS						

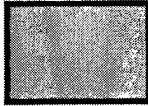
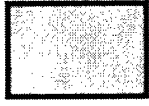
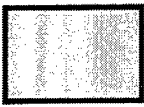
LEGEND:		
ROBUST UTILITY	MODERATE UTILITY	LIMITED UTILITY
		

Table 3-2: IO Utility of SOF Collateral Activities

MISSION/ ENVIRONMENT	INFRASTRUCTURE			PSYCHOLOGICAL		
	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
		

In this chapter, SOF has been examined as a supporting force in a strategic IO campaign. There is also utility in using IO to enhance the effectiveness of SOF. The next chapter will examine the integration of SOF and IO with SOF as the supported force.

IV. THE TACTICAL INTEGRATION OF SOF AND IO

The previous chapter examined the ways in which SOF could support a strategic IO campaign. Conversely, information operations may also support special operations. While IO can contribute to all special operations, the primary focus of this chapter is on combat operations. This chapter will use two concepts, the OODA loop and relative superiority, to help explain how information operations can enhance the chances for success at the tactical level. Specifically, how using information operations to disrupt or manipulate the decision cycle affects the ability of SOF to achieve relative superiority. IO support for extended-duration special operations will also be examined briefly.

A. THE DECISION CYCLE (THE OODA LOOP)

All of the concepts of IO discussed in the second chapter attempt to influence the target audience, either directly or indirectly. A popular model for rational decision making, commonly referred to as an OODA loop, is a useful tool for describing the effects that information operations can have on the decision-making process of the target.

Colonel John Boyd is credited with development of the OODA loop model, first articulated as part of his Asymmetric Fast Transient theory of conflict.¹ "OODA" is an acronym that represents the steps required in a rational decision-making cycle: observe, orient, decide, and act. Boyd originally used the concept in describing how a fighter pilot could gain a decisive advantage over an adversary in combat; the pilot completing the cycle faster than his adversary was able to gain the initiative and control the battle. The

concept has been extended to other applications, including information operations. Although it was originally used to describe individual actions, the process is equally applicable to group actions. It is important to note though that as the scope of application expands, the complexity increases. Beyond the individual level, there may be multiple concurrent cycles operating at any given time. The interaction of these cycles may be difficult to predict or control. The diagram below illustrates the steps that form the cycle.

The first step in the cycle is observation, the process of gathering raw data from

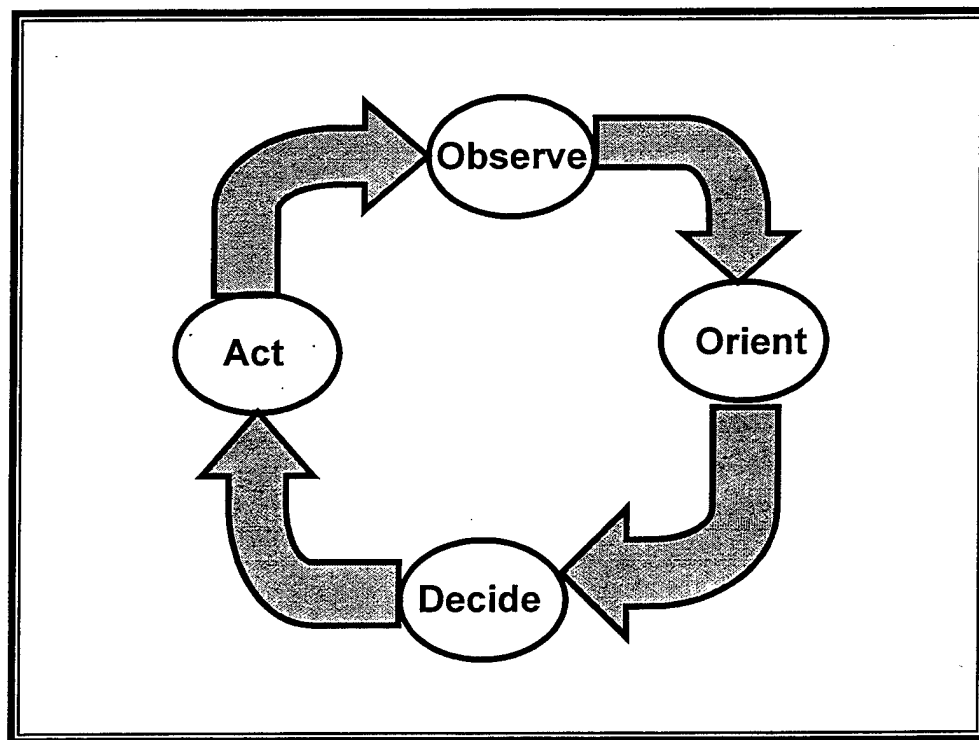


Figure 4-1: Boyd's OODA Loop Model of Rational Decision-Making

the environment. The data does not constitute a situation analysis, only the inputs for that

¹ John Boyd, *A Discourse on Winning and Losing*, Unpublished briefings and essays Air University Library: Maxwell AFB, AL, document M-U 30352-16, no. 7791. August 1987.

analysis. The “observe” function is not limited to visually acquiring data; the observer’s other sensory functions also provide data. External sensors² can also provide inputs. During the second step of the cycle, orientation, the observed data is processed or mentally synthesized into usable information.³ During this step, the observer forms an initial assessment of the situation. This assessment is a product of not only the raw data gathered but also of the biases of the observer, i.e. his interpretation of the facts. The observer incorporates new data with the existing knowledge of the situation. The “unique personal characteristics such as genetics, culture, and experience” of the observer influence this process heavily.

The next step of the decision cycle is act. The analysis of the situation developed in the orientation step forms the basis for the decision made in this step. The decision-maker weighs the information acquired during the first half of the cycle, considers possible options, and chooses a course of action. Like the other steps of the cycle, the experiences of the observer influenced his ability to make a decision. The final step in the cycle is action; the decision made in the previous step is implemented and the cycle begins again, incorporating the results of the previous cycle.

² The term “sensors” is used in the broadest possible sense. Communications media can be “sensors” since they provide data and information about the outside world to the observer. The same can be said for individuals in a primitive society where information is passed orally.

³ Gregory M Schechtman, *Manipulating The OODA Loop: The Overlooked Role Of Information Resource Management In Information Warfare*. Thesis. Air Force Institute of Technology Air University. December 1996. 35.

B. THE CONCEPT OF RELATIVE SUPERIORITY

William H. McRaven introduced the concept of relative superiority to explain how SOF succeeded against numerically superior foes in well-prepared positions. McRaven defined relative superiority as the “condition that exists when an attacking force, generally smaller, gains a decisive advantage over a larger or well defended enemy.” Three basic properties defined relative superiority:

1. Relative superiority is achieved at the pivotal moment in an engagement.
2. Once relative superiority is achieved, it must be sustained in order to guarantee victory.
3. If relative superiority is lost, it is difficult to regain.

The third property is particularly important to SOF, particularly when engaging a larger conventional force. Although SOF have many weapons at their disposal they can be at a significant disadvantage to conventional forces. This is especially true as the distance to the target increases, reducing the availability of external support. Even precision guided munitions can take a long time to reach a target, a long enough time for a numerically superior force to overrun a much smaller force.

McRaven identifies six “Principles of Special Operations”: simplicity, security, repetition, surprise, speed, and purpose.⁴ According to McRaven, “Relative superiority is gained only through the correct application of all six principles.”⁵ While IO does not offer any benefits for improving repetition or purpose, it can contribute to the other four principles. IO can improve simplicity by reducing the number of targets that SOF must

⁴ William H McRaven, *Spec Ops - Case Studies in Special Operations Warfare: Theory and Practice* (Novato: Presidio Press, 1995) 9-23.

engage. This can be accomplished in a number of ways. For example, deception may be used to divert forces away from the target area or defensive systems may be disabled through infrastructure attacks. IO is also useful for enhancing security, through both psychological and infrastructure means. Improving security also contributes to achieving surprise. Finally, IO can help to slow the enemy's reaction thereby allowing SOF to accomplish the necessary tasks rapidly, without significant interference. The next section will discuss in more detail how disrupting the decision cycle with IO achieves each of these effects.

⁵ McRaven 19.

The figure below depicts a generic relative superiority graph.⁶ The x-axis represents time and the y-axis represents the probability of mission completion. The intersection of these two axes represents the point of vulnerability. McRaven defined this as the point “when the attacking force reaches the enemy’s first line of defense.” The area of vulnerability is “a function of mission completion over time.” Until the mission is successfully completed, friendly forces remain at risk. As friendly forces achieve relative superiority and move closer to mission completion, they become less vulnerable to failure.⁷

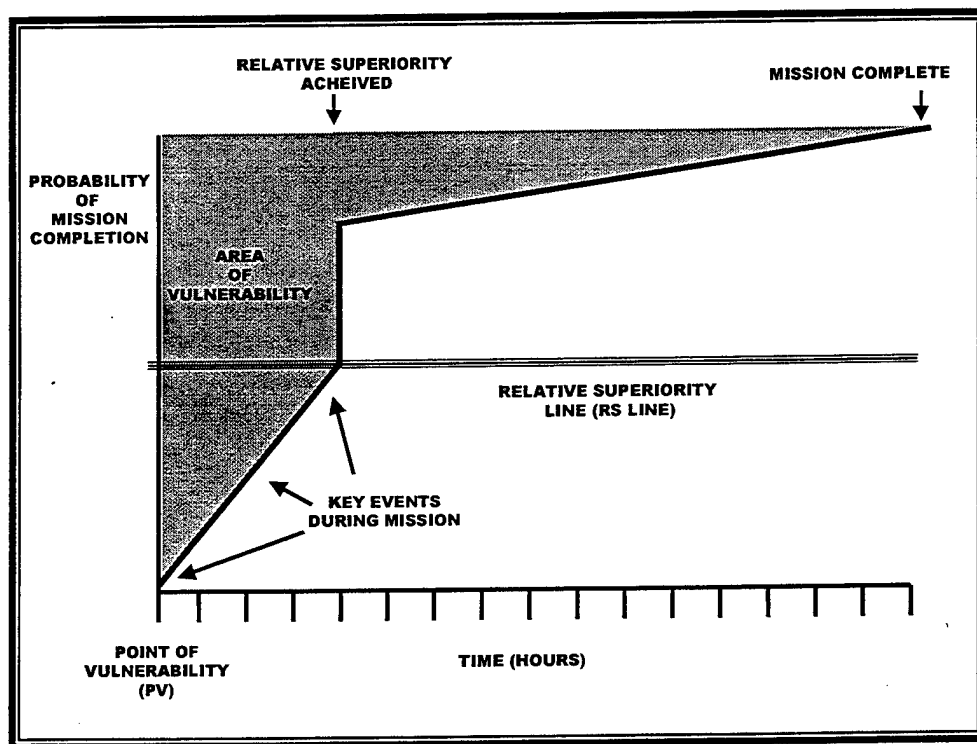


Figure 4-2: Generic Relative Superiority Graph

⁶ McRaven 4-7.

⁷ Ibid. 7-8.

McRaven's area of vulnerability (i.e. mission start point and end) is limited to actions on the objective. In defining the point of vulnerability, he uses "first line of defense" in a very restricted sense, i.e. within range of the enemy's direct fire weapons on the actual objective. He readily admits that this is "somewhat arbitrary." If a broad view of enemy defenses is adopted, the point of vulnerability may exist long before the force is actually on the objective, even before tactical planning begins. For example, if the enemy learns of the operation before execution then friendly forces are vulnerable as soon as they begin planning the operation. They are vulnerable to preemption and other defensive measures, which may include hostile IO. Similarly, by extending the concept of mission completion to include successful exfiltration the area of vulnerability is extended until all forces return to a safe area.

For several reasons, this thesis will use the broader views of these concepts. The first is for the simple reason that IO should be an integral part of an operation from start to finish; restricting the application of IO to the relatively narrow period adopted by McRaven limits or decreases its utility. The expanded view of the area of vulnerability is a valid because of the increased intelligence, surveillance and reconnaissance means available to potential adversaries. Although the threat to operational security has always existed, the rapid communications enabled by advanced technology increases this threat. For example, media coverage of increased activities or potential deployments at a particular base may alert an adversary to an impending operation. High-resolution satellite imagery is also available commercially. Additionally, agents of foreign

governments or other adversaries can disseminate information quickly and securely from almost any location using encrypted e-mail.

Secondly, special operations include more than just destroying or disabling a target. For example, a mission to recover materiel or personnel is a valid special operation. This type of mission is not complete or successful until the return of the recovered item. Additionally, SO which result in large friendly casualties may be classified as strategic failures.⁸ A perfect illustration of this is the ill-fated Task Force Ranger raid in Somalia. Although the raiders were successful in snatching their targets, they could not quickly exfiltrate the prisoners and themselves from the target area. Despite their success in capturing and ultimately exfiltrating their prisoners, the mission was a strategic failure due to the high number of U.S. casualties. This example also illustrates well the necessity for sustaining relative superiority and the difficulty of restoring it once it has been lost.

Accepting the expanded area of vulnerability affects the first principle of relative superiority. Since the area of vulnerability is not limited to actual engagement, it is theoretically possible to achieve RS before an engagement begins, which McRaven acknowledges.⁹ The opposite is also true; it is possible to lose RS before the engagement even begins. The other principles remain unaffected by this change.

⁸ Given the apparent aversion to casualties, it is also possible that a mission that achieved all its objectives could still be classified (by some) as a strategic failure if it resulted in significant casualties to U.S. forces. See Shlomo Gazit, "Risk, Glory, and the Rescue Operation," *International Security* Summer 1981 Vol. 6 No.1: 129.

⁹ McRaven 4.

C. USING IO TO ACHIEVE AND SUSTAIN RELATIVE SUPERIORITY

The decisions made by an adversary have a direct effect on the ability of SOF to accomplish their mission successfully. The enemy's decisions, and the speed with which they are made, can allow him to gain the initiative. This poses a threat to relative superiority. Conversely, delaying the adversary's ability to complete any step in the decision cycle may result in a decisive advantage for the attacking force. Information operations can affect both the outcome and the speed of the decision cycle by degrading or disrupting any step of the cycle. The Department of Defense considers the tactical application of IO/IW to be command and control warfare (C2W).¹⁰ The concepts described below essentially fit this description.

Time is a critical factor in every step of the decision cycle, especially in fluid environments. While the time and information necessary to come to a decision varies, denying the adversary the ability to gather the minimum essential information increases the time required to make decision. As greater amounts of time are required to gather information, the opportunity to make a timely decision is lost. A delay in any step may result in an action that is no longer appropriate, since the situation may have changed. This delay may also allow the problem to become unmanageable and grow to crisis proportions.¹¹ By preventing or delaying a decision and subsequent action, it is possible to gain relative superiority. Therefore, it is useful to look at means to disrupt or manipulate an adversary's ability to make and execute decisions.

¹⁰ Please refer to the glossary in Appendix A for the full definition from *DOD Joint Publication 1-02, DOD Dictionary of Military and Associated Terms*.

Although disrupting any step may have a disruptive effect on subsequent steps, this may not always be the case. For example, although observation may be slowed, the observer may complete the other steps in the cycle rapidly once he has observed the minimum essential data. The same analysis applies to the remainder of the cycle. This implies that it is not the absolute speed of the cycle but the speed of the cycle in relation to the adversary that is important. This is commonly referred to as “operating within the enemy’s decision cycle.”

It is important to note that disrupting one step of the cycle may produce similar effects on RS as disrupting another step. For example, denying the ability to orient and denying the ability to decide may both result in an extension of relative superiority; this is because each step influences the next step. The sections below will examine specific applications of IO to disrupt or delay the steps of the decision cycle and the subsequent effect on relative superiority.

1. Observe

IO provides multiple means to denying the enemy the ability to observe. This is essential to maintaining both security and surprise, which are essential for any special operation.¹² Both offensive and defensive IO can contribute to this objective. Additionally, both the psychological approach and infrastructure attacks are useful for denying or disrupting observation.

¹¹ Schechtman 37.

¹² McRaven 8-23.

Operational security is the most important defensive IO function during the planning phase of the operation. A failure to provide operational security poses catastrophic risks. The area of vulnerability is increased and the probability of mission completion nears zero; relative superiority is near impossible to achieve. Both strategic and tactical deception can contribute to disrupting the adversary's ability to observe.

The most obvious offensive use of IO is denial of service attacks on intelligence collection systems and sensors. Disabling or disrupting the systems that provide these inputs can effectively "blind" the enemy. This can be accomplished using malicious software, electronic warfare (to include directed energy weapons), and physical destruction. These same tools can also attack the communications links between the sensor and the observer. Yet, it is not necessary to disable the external sensors or communications completely in order to achieve an effect. Psychological operations, supported by selected infrastructure attacks, provide another means to deny observation.

The first method exploits an observer's reliance on external sensors. Attacking the sensors in such a way that they appear to be functioning normally, yet provide corrupted data, is commonly referred to as "spoofing." Depending on training and past experiences, the observer may be biased towards the external sensors, i.e. he is more inclined to place more faith in the external sensors than his own senses. An example of this is a pilot suffering spatial disorientation. His past experiences have shown him that the external sensors provide a truer picture of his orientation than his own bodily senses. Therefore, he will rely on those sensors when he has doubts about his orientation. If the sensors appear

to function normally and prove the expected data, the observer may disregard other observations that do not agree with his expectations.

Conversely, someone accustomed to frequent malfunctions of an external sensor may rely more heavily on their own senses. A second method involves creating doubt about the reliability of the sensors; convincing the observer that reliable data coming from external sensors is incorrect. IO could be used to cause periodic malfunctions in the sensors. The desired effect would be to undermine the observer's confidence in the sensors and disregard their inputs. While the techniques used against the sensors are

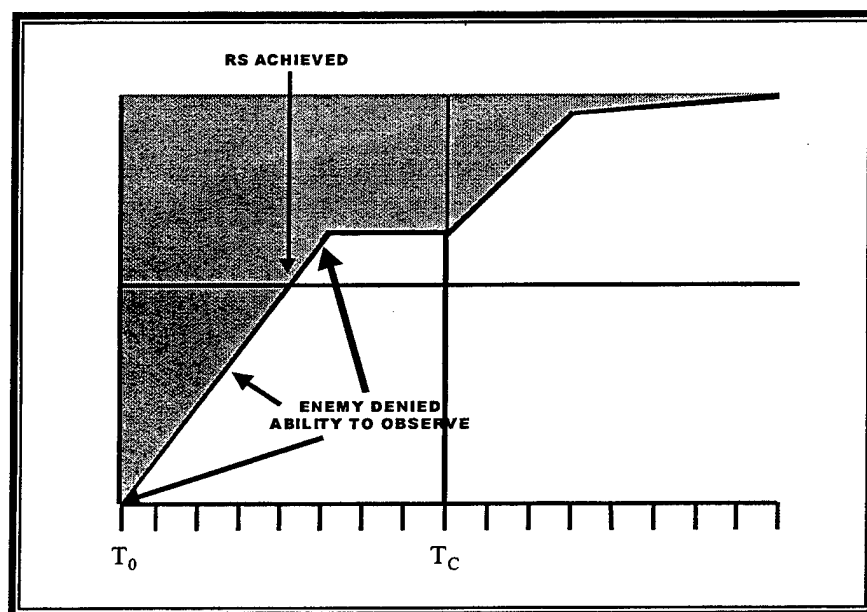


Figure 4-3: RS Achieved before Mission Execution

nearly identical, the essential difference between these two approaches is the timing. In order to undermine confidence in the sensors it is necessary to begin the attacks well in advance of the actual tactical operation. It is also necessary to attack the sensors with

enough subtlety that the attacks are not discovered. This could result in improved safeguards or modifications to the sensors.

The cumulative effect of these actions on relative superiority is straightforward: it can be achieved before the operation even begins. This also reduces the area of vulnerability. If the intelligence provided to the attacking force is accurate, they should have a significant advantage, i.e. relative superiority. McRaven correctly notes that "surprise is essential, but it should not be viewed in isolation."¹³ Surprise cannot compensate for poor intelligence, planning, or execution. Nonetheless, it can contribute significantly to relative superiority. Even if the enemy is well prepared, he is at a disadvantage because the attacking force has the initiative. An enemy unable to observe preparations for an attack is not able to take any additional steps to prepare. He cannot take pre-emptive action against an operation of which he is unaware.

2. Orient

As noted in Chapter II, orientation is arguably the most important step in the cycle because it can affect both what we observe and how we decide. Our experiences shape how we select the data to draw a mental picture of the situation and how we construct that mental picture. This has an immediate effect on the decision step. If the observer is unable to orient, e.g. the situation is unfamiliar or the observed data does not fit the observer's expectations, he may decide to gather more information. Any discrepancy

¹³ McRaven 19.

between observed data and the observer's expectations must be accounted for either by revising the expectations or validating the observed data.¹⁴

There are several approaches to disrupting the ability to orient. The first approach is indirect; it is an extension of "blinding" the enemy. By denying him information upon which he can orient, he is relegated to searching continually for more information or making an uninformed decision. The complement to the first approach is to flood the observer with conflicting data. In theory, it is also possible to overwhelm an adversary with so much data that he cannot successfully orient. He is unable to sort the large conflicting data and must constantly search for more data that will validate a course of action. Consequently, he may be unable to take meaningful action. Interestingly, the same IO tools can be used for either approach: deception, computer network attack, or EW. For example, EW may be used to jam sensors that use the electromagnetic spectrum or it may be deceive the sensors, creating multiple conflicting images.

¹⁴ Schechtman 35.

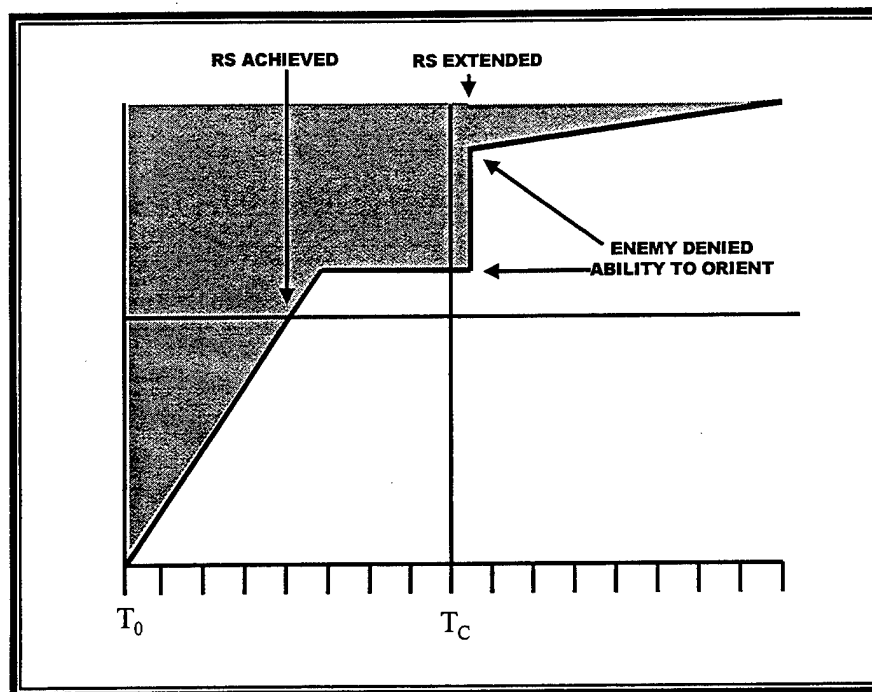


Figure 4-4: Expanding Relative Superiority

Another way to slow or degrade orientation is by presenting the observer with unfamiliar situations. Many adversaries consider and plan for multiple scenarios; to reduce the time necessary to react, they standardized their actions for each scenario. If the situation is unfamiliar or no plan exists, it may take longer to make a meaningful decision.¹⁵ This may be especially true against opponents with highly centralized decision-making and authority. (As noted above, the decision may be simply to gather more data.) Again, deception, computer network attack, and EW can all contribute to this effort, either separately or as part of a larger psychological operation.

¹⁵ This is also an implicit call for tactical and doctrinal innovation to slow an adversary's reaction.

A third approach to denying the adversary the ability to orient correctly involves exploiting or manipulating the biases of the observer. The process of reconciling observed data with existing biases suggests that observed data, even if it is not representative of the actual situation, may be more easily accepted if it conforms to expectations. One possible result is that the observer orients only on the observed data that conforms to his expectations (a cognitive bias). A psychological approach to IO, supported by infrastructure attacks, can present the observer with information that conforms to his expectations. This can delay or prevent orientation to the actual situation and provide friendly forces with an advantage.

The preparations for D-Day offer a potent example of this type of strategic deception. Allied forces conducting Operation Bodyguard were aware of Hitler's belief that the invasion would come at Pas de Calais and they presented information, through multiple channels that reinforced this belief. The allied planners did a masterful job of exploiting the German biases; even after the invasion of Normandy, the Germans remained convinced that the "real" invasion would occur according to their expectations. Their expectations, confirmed by misleading information presented by the Allies, prevented the Germans from immediately recognizing (or orienting on) the threat posed by Operation Overlord. The delay in responding to the invasion of Normandy provided the Allies the time necessary to secure their foothold on the continent.¹⁶

¹⁶ William B. Breuer, *Hoodwinking Hitler: The Normandy Deception* (Westport: Praeger, 1993).

Although smaller in scale, a similar strategic deception can help SOF achieve tactical objectives by delaying the adversary's ability to orient once an operation is underway. Denying an adversary the ability to orient can help to achieve or expand relative superiority. For example, the graph below shows a hypothetical situation where the attacking force has achieved relative superiority before mission execution. Once on the objective the enemy observes them but he is unable to orient because information operations have led him to believe that the attack would occur elsewhere. While he struggles to orient, the attacking force is able to exploit the confusion and quickly position itself for success.

3. Decide

There are three approaches to disrupting the decision step: prevent a decision altogether, compel a decision that is counter-productive, or simply slow the adversary's decision. It is difficult to prevent a decision completely, since even inaction can be construed as a decision not to act. The key is preventing decisions that adversely affect the conduct of the mission or forcing decisions that are not beneficial to the adversary.

The same IO techniques used to disrupt or prevent observation and orientation are also effective for delaying a decision. If the enemy is unable to accomplish either observation or orientation, he will be unable to make an informed decision quickly. These same techniques can also force a counter-productive decision. For example, deception and psychological operations can create the illusion of a threat to another target and force an adversary to commit forces that would otherwise be available to defend the actual target.

Disrupting the decision step can help sustain or extend relative superiority. Relative superiority is sustained when the enemy is unable to effectively counter the actions of the attacking force; it is extended when the enemy makes decisions that result

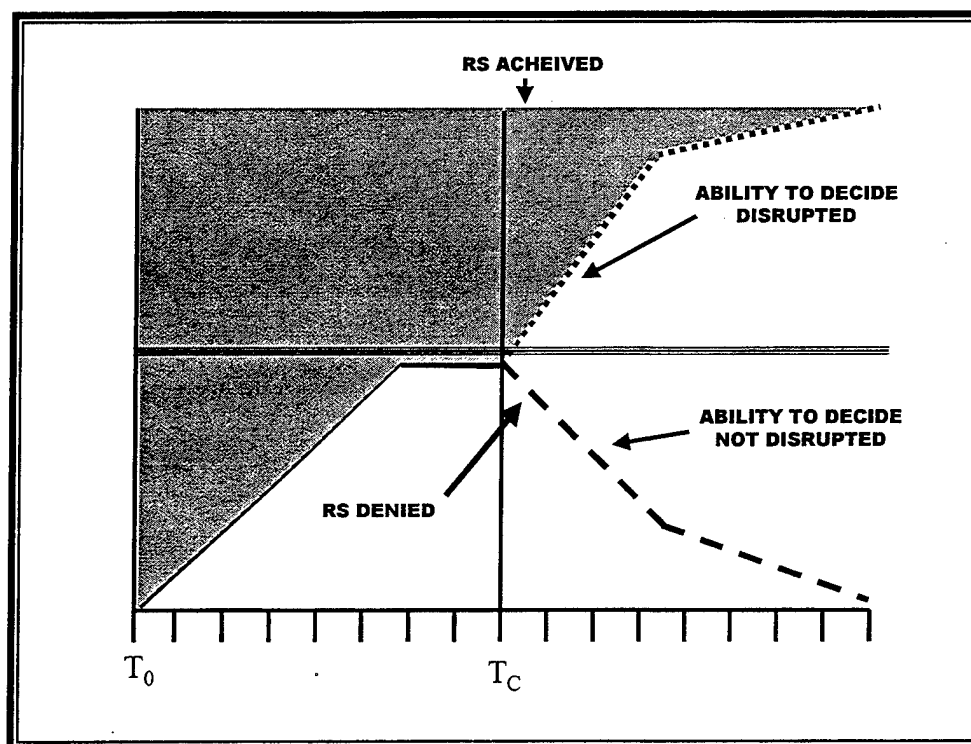


Figure 4-5: Sustaining Relative Superiority

in counter productive actions. The graph above illustrates two possible outcomes resulting from the enemy's decision. The solid line on the top is the result of delaying or preventing an effective decision; this allows the attacking force to conduct operations without effective resistance. The slope of the line after contact is dependent on the relative speed of the decisions of both parties. As the enemy decision is slowed or the speed of friendly forces increases, the slope increases (i.e. relative superiority is extended more rapidly). Conversely, the slope decreases as the enemy decides more quickly or the attacking force moves more slowly. Although the attacking force has achieved relative

superiority before execution, it is still possible to lose it. The dashed line on the bottom illustrates a possible result of this interaction.

4. Act

As with each previous step, disrupting any of the preceding steps can disrupt the remainder of the cycle. This is implicit in the sequential nature of this process. However, the enemy's ability to act can also be attacked directly. Isolating the decision-maker from those who must carry out the decision is another means to delay action. The decision maker may be able to observe, orient, and decide without interference but still be unable to act. The infrastructure approach is useful for isolating a commander from his forces by severing communications links. Severing the links between units can prevent a coordinated response. Another method is to use directed energy weapons to disable weapons and transportation systems. EW and computer network attacks are well suited to this type of attack (denial of service). They may also be used to attack the integrity of orders by altering the contents of messages or simulating communications.

When the decision-maker is physically located with those who must carry out his decisions, it is difficult to disrupt his ability to communicate. Yet, the ability of a commander to act can still be degraded using psychological operations, which are useful for undermining confidence in a commander. Psychological operations can also adversely affect the morale of enemy soldiers; this can directly undermine their will to fight.

Each of the actions described above can contribute to disrupting the enemy's ability to act. The disruption may be total, but is more likely to be only partial. Under most circumstances, an adversary will retain some residual ability to act, even if only in

small, disorganized groups. Nonetheless, the inability of an adversary to act decisively will invariably lead to relative superiority. In graphical terms, the effects of this are identical to the inability to decide. The greater the degree of disruption, the more rapidly relative superiority will increase. Decisive action by the adversary can lead to a rapid decrease in relative superiority.

An interesting implication of this dynamic is that equilibrium between the decision cycles of the two forces will result in an RS line with a slope of zero. This means that the force with relative superiority at the start of an engagement still has a greater chance of successfully completing the mission, all other factors being equal. This argues strongly for attempting to achieve relative superiority before executing the mission.

D. IO SUPPORT FOR EXTENDED-DURATION SPECIAL OPERATIONS

Although highly useful, McRaven's Theory of Special Operations is limited to short duration special operations, i.e.-combat actions. However, there are a number of special operations that occur over an extended period. Extended special operations include a variety of missions. The most obvious is the unconventional warfare (UW) mission. Other special operations that may fall into this category include Foreign Internal Defense (FID), and some SOF collateral activities, i.e. peace operations, counter drug efforts, humanitarian assistance, and humanitarian demining.¹⁷

¹⁷ Combating Terrorism (CBT) and Counter Proliferation (CP) may also be considered extended operations. These missions are extended-duration efforts, which include a variety of efforts, most conducted in conjunction with other military organizations and government agencies, but the tactical role of SOF is mostly limited to DA and SR. For example, an attack on a WMD facility or a terrorist organization is the culmination of a protracted, interagency effort. However, SOF is not principally

1. Sequential and Cumulative Strategies

The concept of a cumulative strategy is useful for thinking about IO support for extended duration special operations. Admiral J.C. Wylie introduced the concepts sequential and cumulative strategies in 1952. A sequential strategy represented the traditional strategic view of major military campaigns. Strategists considered campaigns as "a series of discrete steps, or actions, with each one of this series of actions growing naturally out of, and dependent upon, the one that preceded it."¹⁸ the result of each step alters the conduct of the remainder of the campaign; if any action fails, the outcome of the entire campaign is affected. Many of the great campaigns of World War II can be analyzed as sequential strategies.¹⁹

Conversely, a cumulative strategy consists of a "collection of lesser actions...not sequentially interdependent." The outcome of the campaign is dependent upon the cumulative result of these lesser actions. The outcome is the "less perceptible minute accumulation of little items piling on top of the other until at some unknown point the mass of accumulated actions may be large enough to reach to be critical."²⁰ Wylie offers the submarine campaigns of World War II as examples of this type of campaign. He also

responsible for most of the non-tactical tasks associated with these missions. IO support of those tasks for which SOF is principally responsible (i.e. DA and SR) is described in the previous sections.

¹⁸ Joseph C.(J.C.) Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis: Naval Institute Press, 1989) 22.

¹⁹ Ibid. 23.

²⁰ Ibid. 24.

suggests that psychological warfare and economic warfare also well suited for this type of strategy.²¹

Wylie explicitly states that these strategies are not mutually exclusive. Rather, they are usually interdependent. However, according to Wylie, "there is no major instance in which a cumulative strategy, operating by itself, has been successful."²² A cumulative strategy, directed at critical targets and used in conjunction with a sequential strategy, can mean the difference between success and failure.

For IO, the practical implication is that a variety of means should be applied to achieve the desired effect. This is especially true in attempts to influence a target psychologically. As noted in Chapter II, perception and understanding develop over extended periods; altering either is difficult to achieve with a single event. This need for a cumulative strategy may also apply to some infrastructure targets. For example, well-designed computer networks avoid single points of failure; they are inherently robust systems. Additionally, many critical communications systems may have separate backups that must be attacked also. It may take multiple smaller scale attacks on both primary and backup systems to deny service. Likewise, system penetration (for monitoring or corruption) may not occur as the result of a single effort. Many network security systems have multiple methods of intrusion detection, all of which must be disabled or spoofed in order to prevent detection.

²¹ Wylie 23.

²² Ibid. 25.

2. Support for Unconventional Warfare

Unconventional warfare has a variety of requirements that IO can support. First, IO can support direct attacks against government forces in the same manner as short duration SOF missions. IO against selected infrastructure targets can also help undermine confidence in the abilities of the ruling regime. Recall that infrastructure attacks include a variety of means, not only physical destruction. Infrastructure attacks are also useful both for disrupting government propaganda and for disseminating insurgent propaganda. For example, IO may be used to corrupt print and broadcast media, deleting government messages while inserting insurgent messages. In more advanced societies, this may mean penetrating government computer networks and hacking into government web sites or databases. The success of these attacks contributes to the demoralization of the government, its forces, and their supporters. This, in turn, can support the requirements for recruiting an indigenous force and gaining the confidence and support of the local population, which are necessary conditions for success.

A third task is gaining the support of the international community. Regardless of the technological state of the disputed territory, insurgents can also use the Internet and other advanced communications means to garner international support for their efforts. The perception management efforts of the Zapatista rebellion in Mexico have demonstrated the usefulness of disseminating information via the Internet.

This approach constitutes a cumulative strategy; no single event will determine the outcome of the campaign. Rather, the sum of all these efforts determines the outcome. This holds true for both direct attacks on the regime and efforts to gain the support of the

local populace. Insurgents do not have the resources to confront the government directly, even with external support. SOF capable of employing a variety of IO means to the insurgent's efforts can serve as a force multiplier, maximizing the use of limited resources.

3. Support for Other SOF Missions and Collateral Activities

As noted above, FID, CA, peace operations, and humanitarian efforts may require extended duration efforts. With the exception of FID, these efforts do not regularly involve the use of force.²³ Additionally, they are often conducted in areas where the infrastructure has been damaged or destroyed, by either war or natural disaster. A principal goal of each of these operations is to establish control of the local population to facilitate other efforts. At the tactical level, achieving effective population control without the use of force reduces resource requirements and risk to U.S. forces. This suggests that a psychological approach to IO is best suited for these types of operations.

A psychological approach to IO can help improve domestic and international support for the host nation government and U.S. involvement. Conversely, it can be useful for discrediting forces opposed to either of these entities.²⁴ U.S. efforts in Somalia, Bosnia, and Haiti are excellent examples of the type of environment where this approach

²³ Many of the engagement activities of SOF are frequently and mistakenly referred to as FID. They do not regularly involve protecting the host nation government from "subversion, lawlessness, and insurgency," which often involves the use of force. In reality, many of these activities are more appropriately classified as Security assistance missions.

²⁴ Department of Defense, *Joint Pub 3-53, Doctrine for Joint Psychological Operations* (Washington, D.C.: GPO, 1996) V-5.

can directly affect tactical operations.²⁵ In these types of situations, IO can help shape the perceptions of the various factions involved in the disputes. For example, while IO may not be able to change the Bosnian Muslims' perception of the Serbian leadership, it can help to create a perception of the United States as an honest broker, interested only in a peaceful and equitable solution. A more successful effort to generate popular support in Somalia may have precluded the resentment that the U.S. presence eventually generated. Although some singular events can alter perceptions, it is difficult to plan, implement, and anticipate the consequences of this type of event. A cumulative strategy, employing all elements of information power at the disposal of the U.S., is more likely to achieve the desired result.

E. POST MISSION IO SUPPORT

Because of the strategic and political nature of special operations, it is important to consider what happens after an operation, particularly if it has ended in failure. Domestic and international reaction to a mission can undermine the strategic benefits generated by the mission. Psychological IO can be useful for explaining "the purpose of an operation to counter enemy reaction and ensure that friendly, neutral, and hostile audiences know what has occurred and why."²⁶ This can help to mitigate the adverse impact of mission failure. In cases of tactical success, the results of the mission may be

²⁵ This is not an evaluation of how well the U.S. applied IO in these situations; it is only a statement that the psychological approach to IO can be useful in these types of situations.

²⁶ DoD, *Joint Pub 3-53*, V-7.

exploited to demoralize other potential adversaries. In some cases, regardless of outcome, IO can be used to deceive selected audiences about the intent and results of the operation.

F. THE ADVANTAGES OF INTEGRATION

Using IO to support special operations offers the advantages of economy of force – successful IO can reduce the number of forces necessary to accomplish a mission. This holds true regardless of the length of the operation. For short duration missions, IO support can help to achieve and sustain relative superiority. For extended duration operations, IO can help to achieve popular support and cooperation. In both instances, this may translate into a smaller force requirement than attempting the mission without IO support. Because the unilateral employment of SOF generally provides economy of force, the successful integration of IO creates the opportunity for even greater economy.

IO support for SOF also offers the potential for reducing risk, both physical and political. By improving economy of force, IO can reduce the number of troops that must be placed in harm's way. This directly affects political risk since the number of casualties is a factor in determining political success. The application of IO to post mission perception management can also reduce political risk by helping to ensure the support of domestic and international audiences.

G. SUMMARY

This chapter reviewed the concept of an OODA loop and expanded the concept of relative superiority. It examined the means available to disrupt the OODA loop in order to achieve, extend, or sustain relative superiority. Both the psychological and infrastructure

approaches to IO offered multiple means to disrupt and degrade the enemy's decision cycle. By slowing the relative speed of the enemy's decision cycle, IO can allow SOF to operate with the initiative, to be one step ahead of the adversary. Even when the enemy has well prepared defenses and contingency plans, IO can frustrate their implementation. This may provide the crucial time and space for SOF to achieve their mission.

IO support for extended-duration special operations was also examined. While short duration operations are well suited to a sequential IO strategy, extended-duration operations benefit from the use of a cumulative strategy. Although these strategies are not mutually exclusive, a cumulative strategy is more appropriate for extended duration operations. This is particularly true of the psychological approach to IO since perception and understanding usually develop over long periods. Further, a psychological approach to IO may be the best option for primary SOF missions and collateral activities where the infrastructure is non-existent or severely damaged.

The previous chapters have examined the integration of SOF and IO in light of the current capabilities of SOF. The next chapter will briefly examine the impact of this integration and the changing security environment on future roles and missions for SOF. This is a contentious issue not only for SOF but for the services as well; evaluating roles and missions, both new and old, is essential to the future utility and viability of SOF.

V. THE FUTURE OF SOF ROLES AND MISSIONS

A rapidly changing world deals ruthlessly with organizations that do not change – and USSOCOM is no exception.¹

General Peter J. Schoomaker
CINC USSOCOM

While General Schoomaker's warning is no doubt true and valuable advice, it is also good to remember that while all change is change, not all change is progress. Change is necessary to maintain relevancy in an evolving environment. Yet, identifying the appropriate changes necessary to remain viable in future environments is a difficult task, particularly when there is a high level of uncertainty. This subject is extremely complex; changes in roles and missions may have far reaching implications for recruiting, doctrine, training, leader development, organization, and acquisition. The potential costs of failure are high:

SOF's ability to distinguish between appropriate and inappropriate new roles and missions...will decidedly impact...its viability as an instrument of national policy.²

Because of this, a single chapter of this thesis could not possibly do justice to the subject. However, it is possible to examine the integration of IO with respect to the future of SOF. Should IO be a principal mission for SOF? Is SOF well suited for IO or is it better suited to its traditional roles and missions? What are the implications of integrating SOF and

¹ Peter J Schoomaker, "U.S. Special Operations Forces: The Way Ahead." *Special Warfare* Winter 1998: 8.

² Richard H. Schultz, Jr., Robert L. Pfaltzgraff, Jr. and W. Bradley Stock. *Roles and Missions of SOF in the Aftermath of the Cold War*. (Medford: Fletcher School of Law and Diplomacy, 1994) 197.

IO? This chapter will examine the risks and benefits of integrating SOF and IO. It will first explore the roles and missions debate, including the current roles and missions of SOF. Next, it will evaluate whether IO is an appropriate mission for SOF. Finally, it will examine some of the potential ramifications of accepting IO as a principal SOF mission.

A. THE ROLES AND MISSIONS DEBATE

The issue of roles and missions is fundamentally important to national security and has been the subject of a great deal of debate; it requires careful examination. This issue is particularly important to SOF because of the increased demand for their services and competition from the other elements. Chapter I highlighted several factors driving changes in the security environment, including new threats, constrained resources, and a potential RMA. This has led to a change in either priority or relevance for many roles and missions, which directly influences the allocation of resources. An organization's attempt to ensure its survival will force it to compete for these resources. Therefore, in this era of restricted resources, SOF must compete with conventional forces, not only for resources but also for roles and missions.

The nature of current commitments and limited resources do not allow SOF to take on new roles and missions *ad infinitum*. Doing so threatens the ability to respond to both current and future threats. Each new mission places more demands on the limited resources and reduces the ability to tackle emerging threats. Conversely, a consistent rejection of new roles and missions may lead decision-makers to turn to conventional forces. The demand for forces with SOF skills may also tempt conventional forces to duplicate SOF skills in order to secure additional resources. This threatens the very

existence of USSOCOM. In fact, some have expressed doubt as to whether SOF and USSOCOM are really needed any longer:

High-tech surveillance systems and long-range precision munitions...are reducing the need for the "direct action" missions which are the forte of the special operations community's capabilities. In the future, technology may make it rarely necessary to risk elite troops on hazardous missions to conduct reconnaissance or sabotage. Consequently, with the primary warfighting missions of special operations personnel superseded by technology, it is not clear that it is necessary to maintain their service-like existence as a separate combatant command. As the U.S. Marines have proven with their special operations capable units, whatever residual requirement that may exist to secrete troops deep behind enemy lines (e.g., rescue missions) can be effectively accomplished within the organizational framework of traditional military formations.³

Given the pressures outlined above, USSOCOM has three options available concerning roles and missions:

1. Maintain the status quo – risk being irrelevant or unprepared
2. Accept new roles and missions without discarding existing ones.
3. Accept new roles and missions while discarding some existing ones.

At this point in time, USSOCOM has chosen the second option; new roles and missions have been added while continuing to maintain the stable of existing roles and missions. The details of this will be addressed in the next section.

There are specific risks associated with these options. By maintaining the status quo in the face of a changing environment, SOF risks becoming irrelevant. Worse yet,

³ Charles J. Dunlap Jr., "Organizational Change and the New Technologies of War," Paper presented to the Joint Services Conference on Professional Ethics (JSCOPE) Washington, D.C. Jan 30, 1998. n.pag. Online. Internet. Available: www.usafa.af.mil/jscope/Dunlap98.HTM

SOF risks being unprepared for future threats which could lead to tactical and strategic failure. Accepting new roles and missions while maintaining existing ones threatens to make SOF a "jack of all trades, master of none." Since strategic utility is generally predicated on tactical excellence, this would not bode well for the strategic utility of SOF. Susan Marquis notes the willingness of SOF to accept challenges, whether or not it is appropriate to their capabilities. This translates into "an increased probability of failure as SOF are called upon to conduct operations outside its area of comparative advantage."⁴ Accepting new roles and missions while discarding some or all of the existing ones also entails accepting risk. There is no guarantee that any particular role or mission will be relevant in the future. Nor is there a guarantee that SOF will be able to maintain the same level of performance for new missions.⁵

In addition to the specific risks outlined above, there are some general risks associated with any change in roles and missions. First, duplicating capabilities is a waste of scarce resources. This is equally applicable to SOF and conventional forces; SOF should not duplicate capabilities found in conventional forces and vice versa. Second, assigning SOF missions better suited for conventional forces may cause SOF to lose the unconventional mindset and approach to problems that has contributed to the remarkable

⁴ Susan Marquis, *Unconventional Warfare: Rebuilding U.S. Special Operations Forces* (Washington, D.C.: Brookings Institution Press, 1997) 263.

⁵ The quality of SOF should go a long way toward eliminating this last threat but it is impossible to eliminate it altogether. At the very least, there will be a learning period during which performance may suffer.

success of SOF.⁶ This loss of distinct capabilities/roles may also lead SOF to become “conventionalized,” robbing SOF of their *raison d’être*.⁷ The benefits of “getting it right” are obvious. Properly assigned roles and missions reduce duplication, which provides an economical use of resources. It also ensures continued relevance and viability for SOF.⁸

B. THE ROLES AND MISSIONS OF SOF

Before looking at new roles and missions, it is important to understand the traditional and existing roles and missions. Every component of the armed forces, including SOF, has a particular role to play in the national security strategy. When assessing roles it is not sufficient merely to say that SOF provide military capabilities that are not available elsewhere in the armed forces. This is simply too broad and risks creating an environment where SOF assume responsibility for every mission that conventional forces cannot or will not do. The roles must be specifically defined to reduce the temptation for misuse.

According to Christopher J. Lamb, SOF has traditionally played “two broad, enduring roles,” that of the commando (in direct action missions) and the unconventional warrior (in UW, FID, Psyops, and CA missions). Lamb states that SOF operate in the commando role when they execute “precision penetration and strike operations in limited,

⁶ Marquis 262-263.

⁷ Christopher J. Lamb, “Perspectives on the Emerging SOF Roles and Missions: the View from the Office of the Secretary of Defense” in *Roles and Missions of SOF in the Aftermath of the Cold War*, Richard H. Schultz, Jr., Robert L. Pfaltzgraff, Jr. and W. Bradley Stock, eds. (n.pub., 1994) 206-207.

⁸ Lamb 206-207.

specialized contingencies across the conflict spectrum.” These are normally short duration, direct action missions. Conversely, they operate in the unconventional warrior role when they “influence, advise, train, and conduct operations with foreign forces and populations.” The unconventional warrior role emphasizes language skills and cultural and political sensitivity; it tends to require “patient, long-term commitment.” Because psychological operations and civil affairs involve influencing foreign forces and populations, they are included in Lamb’s concept of the unconventional warrior role.⁹

Both of these roles were important during the Cold War. Although SOF continues to play these roles, the end of the Cold War has added roles and missions to the SOF portfolio. USSOCOM refers to the role of SOF as “warrior diplomats,” which reflects their role in peacetime as well as war.¹⁰ While this is useful in some contexts, it is insufficient as a complete description of the actual roles currently played by SOF. The discussion below offers an expanded description of the actual roles and missions.

The traditional role of the commando remains but it has expanded to include counter-proliferation (CP) of WMD, combating terrorism (CBT), and combat search and rescue (CSAR). These are all natural extensions of SOF capabilities. CSAR is actually designated a collateral activity. SOF participates in these activities, which take advantage of SOF capabilities but are not principal missions. Collateral activities are frequently conducted in conjunction with conventional forces.

⁹ Lamb 201.

¹⁰ USSOCOM, *1998 Posture Statement* 6.

Because SOF routinely conducts collateral activities, they constitute an important resource requirement. Therefore, any discussion of roles and missions should consider collateral activities. Additionally, a change in SOF capabilities dictated by a change in roles and missions could adversely affect the conduct of these activities. Assuming that these activities are important to the national security strategy, any change in the roles and missions of SOF may require other forces to accept these missions.

Lamb's "unconventional warrior" has become the "diplomat" in recognition of the application of SOF capabilities across the spectrum of conflict. However, this is no longer a singular role. In reality, the "diplomat" role consists of three separate roles: regional engagement, humanitarian assistance, and law enforcement support. The missions that support the later two roles are primarily collateral activities. The exceptions are civil affairs (CA) and psychological operations (Psyops) missions.

The regional engagement role closely resembles Lamb's unconventional warrior. The primary difference between the unconventional warrior and regional engagement roles is the additional of the security assistance and coalition support missions. Each of these roles makes use of traditional SOF strengths such as language skills and cultural/political sensitivity. The coalition support mission has taken on added significance since the Gulf War. As the U.S. increasingly looks for multinational participation and support, SOF has become the force of choice to monitor and support foreign forces.

Although the regional engagement role is officially only a concept, it accurately describes a role that SOF is currently playing. A concept paper prepared for U.S. Army

John F. Kennedy Special Warfare Center and School describes three functions provided by regional engagement forces: situational awareness, battlespace preparation, and war avoidance. SOF accomplish these functions in the context of existing missions and collateral activities.

The regional engagement role allows SOF to serve as an additional source of intelligence while actively assisting allies. SOF provides situational awareness by gathering human intelligence (HUMINT). They can observe and interpret conditions, attitudes, actions, and capabilities in the course of conducting other activities. Their presence also allows them to accomplish the other functions. The intelligence provided contributes to plans to defuse potential crises. SOF also act as force multipliers by enhancing the readiness of the host nation forces. Finally, if a confrontation is unavoidable, SOF forces in a regional engagement role help prepare the battlespace for conventional forces. Battlespace preparation can take different forms, many of which can occur long before a crisis is imminent. For example, it may include actions designed to increase interoperability between U.S. and host nation forces.¹¹

The humanitarian assistance role is another recent development. Again, it seeks to capitalize on SOF language skills and cultural/political sensitivity. The ability of SOF to deploy rapidly and operate in austere environments is also a plus. Finally, the role of law enforcement support, particularly in counter narcotics efforts, has also been given to SOF.

¹¹ Research Planning Associates, *Regional Engagement: A Concept Paper*. n.pub. : 9-13.

Neither the humanitarian assistance or law enforcement support roles are the exclusive domain of SOF. Conventional forces also perform missions associated with this role.

Table 5-1: Traditional and Current Roles and Missions of SOF

	ROLE	MISSIONS/COLLATERAL ACTIVITIES
TRADITIONAL	Commando	DA, SR
	Unconventional Warrior	UW, FID, CA, PSYOPS
CURRENT	Commando	DA, SR, CBT, CP, CSAR
	Regional Engagement	FID, CA, PSYPOS, SA, CS
	Humanitarian Assistance	CA, PSYOPS, HA, HD, PO,
	Law Enforcement Support	CD

C. ACCEPTING IO AS A MISSION FOR SOF

Is IO an appropriate mission for SOF? USSOCOM has already included IO in its list of primary missions, using this definition:

Actions taken to achieve information superiority by affecting adversary information and information systems while defending one's own information and information systems.¹²

This is identical to the definition provided by *Joint Pub 3-13 Information Operations*. Chapter II categorized this as primarily an infrastructure approach. Chapter II also identified a psychological approach as a concept of information operations. These concepts are not mutually exclusive, but they have different implications. For example,

adopting the psychological approach may mean that there is no discrete set of operations that constitute information operations. Any operation can be designed to have a psychological impact. In that case, it may be unnecessary to list IO as a primary SOF mission. Chapter III noted the numerous ways that existing SOF missions support the psychological approach. Any new SOF missions to support the psychological approach would probably be oriented on infrastructure attacks. Regardless of the chosen approach to IO, it is likely that SOF would conduct selected infrastructure attacks. Adopting the infrastructure approach would have a more significant impact on the roles and missions of SOF. Therefore, this analysis will focus on the suitability of IO as a SOF mission based on the infrastructure approach.

1. Criteria for New Missions

What are the criteria for evaluating appropriate missions? Christopher Lamb suggests some basic guidelines for evaluating current and future SOF missions. His definitions of traditional SOF roles provide the basis for these guidelines. If mission success depends on the use of SOF (either as commandos or unconventional warriors), the mission should be a primary SOF mission. This is another way of stating that mission success is dependent upon application of SOF core competencies. Missions that other forces can accomplish, but which have a significantly higher prospect of success with SOF participation, should be collateral activities for SOF. If the chance of mission success is only marginally higher when SOF perform the mission, it should be assigned to

¹² USSOCOM, *1998 Posture Statement* 3.

SOF only in exceptional cases. Finally, Lamb holds that any mission that conventional forces can successfully accomplish is not an appropriate mission for SOF; duplication of capabilities is not an efficient use of resources and invites misuse.¹³

Lamb's criteria are an excellent starting point for evaluation but they require some refinement. They are rightly focused on the bottom line of mission success, but only with respect to single missions. In particular, Lamb does not consider the impact of new missions on the ability to carry out existing missions. At the very least a new mission should not undermine the ability of SOF to execute other assigned missions. Ideally, any new mission would enhance the ability to execute other missions.

An additional criterion should address the strategic benefit of the mission. SOF provide a valuable strategic asset; their abilities should be employed to gain a strategic advantage. Even missions that require a commando capability may not generate a strategic advantage. Therefore, it would be a waste of a valuable resource to assign SOF missions without strategic relevance.

The restated criteria for evaluating the propriety of a mission for SOF are listed below:

- SOF core competencies should be essential to mission success
- A SOF mission should not duplicate capabilities resident in conventional forces.
- A new mission must not adversely affect the ability of SOF to execute current missions.
- The mission should contribute to realization of strategic objectives.

¹³ Lamb 206-207.

2. Evaluating IO as a SOF Mission

A brief analysis indicates that IO is an appropriate principal mission for SOF, according to these criteria. It builds on existing core competencies and can support all of the existing roles that SOF play in the national security strategy. A caveat is necessary, though. IO is a broad mission area and it is highly unlikely that it will be the exclusive province of SOF. It is more likely that SOF will conduct only selected IO. Chapter III discussed how SOF core competencies contributed to specific IO missions. With respect to the infrastructure approach, SOF core competencies were essential for infrastructure attacks and certain types of special reconnaissance in isolated or denied areas. These capabilities are not duplicated in the conventional force. The issue of strategic utility was also addressed in Chapter III. It is a well-established fact that SOF, when properly employed, can have considerable strategic effect. Of course, strategic effect is contingent upon employment, but the concepts of information presented in Chapter II are principally strategic concepts.

Evaluating the impact on the ability of SOF to execute other missions is not as straightforward. It is contingent upon resources and the demand for other missions. On the surface, IO does not appear to be a resource intensive enterprise for SOF. Infrastructure attacks or special reconnaissance missions for IO will have mission profiles similar to existing missions. However, IO could consume an inordinate share of resources if the capacity of SOF to perform this type of mission exceeds demand. This is a possibility with new missions where everybody wants "a piece of the action" rather than conducting more mundane existing missions. There are two potential solutions to this

problem. One is to control the capacity to conduct IO; not every SOF unit need be trained or equipped to conduct this mission. A second solution is to hand off other missions that other forces can successfully execute. This is easier said than done for a variety of reasons, including bureaucratic politics. Although some collateral activities may be good candidates for this option, it is beyond the scope of this thesis to evaluate which missions or activities should be discarded.

3. Preparing SOF to Conduct IO

The ancient warrior, now wielding a bronze piercing axe and wearing a helmet of Electrum, must face not only enemy champions, but a host of smaller, more subtle and more elusive foes whose objectives are not always apparent. The excellence of this hero's weapons and his strength and skill in using them still count, but he and his smith must anticipate major changes in the weaponry which he can expect to be used against him and those he is sworn to protect.¹⁴

Sir Michael Howard

Howard's eloquent statement applies goes to the heart of the one of the challenges facing SOF, anticipating and understanding the new weapons of the information age. The most significant challenge facing SOF in preparing for IO will be the development of the technical knowledge regarding advanced information systems. This is a difficult task for several reasons. First, there is a wide variety of systems in use throughout the world, many using different technologies. Achieving some of the desired objectives of IO (e.g. covert penetration of a network) requires specific knowledge of the system. For example,

¹⁴ Sir Michael Howard and John F. Guilmartin, Jr., *Two Historians in Technology and War* (Carlisle Barracks: Strategic Studies Institute, 1994). n.pag. Online. Internet. Available: carlisle-www.army.mil/usassi/ssipubs/pubs94/2hist/2histtc.htm

a denial of service attack may require accessing a router's operating system. These operating systems are usually proprietary and require significant training to understand fully. Acquiring a basic understanding of telecommunications networks or other infrastructure targets is a time consuming task. Developing expert knowledge on a variety of different systems is even more challenging. While some may question the need for SOF to develop expert knowledge, it is useful to remember that SOF usually operate in remote areas with little external support. Therefore, SOF must be capable of evaluating targets and conducting operations without external support. This is particularly true of extended duration special operations like unconventional warfare. The continuous introduction of new technology compounds this problem and demands a robust continuing education program.

The educational requirements may pose a challenge for personnel management; it may require a shift in the assessment and selection of SOF candidates to ensure that they are capable of developing the required skills. One possible solution may be to recruit actively individuals who already possess the required skills. A potential drawback of this may be a clash between the warrior culture and individuals recruited principally for their technical skills.

A third challenge facing SOF is the development of advanced weapon systems, particularly directed energy weapons, and surveillance systems for IO. A lack of suitable weapons will restrict the options available for disabling many targets. Sophisticated surveillance systems, e.g. van Eck monitoring devices, suitable for use by SOF are also required. In addition to dedicated funding from MFP-11, USSOCOM also has research,

development, and acquisition (RD&A) authority that allows it to rapidly acquire new technology for use by SOF. While other agencies and organizations share this burden, it is incumbent upon USSOCOM to support these efforts and make prudent investments in promising systems.

The last challenge involves evaluating SOF doctrine and organization in light of these emerging capabilities. While the general organization of SOF is well suited to many current missions, new organizations may be required to support or conduct IO. It is also possible that some doctrinal changes will be necessary. This is not an argument that changes are absolutely necessary, only that they must be considered.

D. SUMMARY

The issue of roles and missions is contentious; it constitutes both a threat to and an opportunity for SOF. SOF run the risk of becoming irrelevant if they do not adapt to the changing environment. Conversely, the experience and adaptability of SOF present an opportunity to recognize and adapt quickly to emerging requirements. Adopting and integrating IO as a principal SOF mission is a means to ensure continued relevancy without threatening the ability to execute current missions. As discussed in Chapter IV, when properly employed, IO can enhance the overall effectiveness of SOF operations.

Adopting IO as a principal mission will itself pose new challenges for SOF, particularly in the area of doctrine, training, recruiting, and materiel acquisition. USSOCOM is well suited to tackle these challenges. Recall that Chapter III identified adaptability as a core competence of SOF. Organizational flexibility, mature and experienced personnel, and a willingness to try unconventional approaches to problems

all contribute to this ability. The relative independence of USSOCOM, provided by separate funding of SOF activities and RD&A, also contributes to this adaptability.

VI. CONCLUSION

A. SUMMARY

The stated purpose of this thesis was to investigate the relationship between Special Operations Forces (SOF) and Information Operations (IO) and the potential for combining them to optimize limited resources. Chapter I laid the groundwork for the thesis by examining the international security environment, the revolution in military affairs, and the continued demand for SOF. The security environment is changing and uncertain, but there will be continued threats to U.S. interests. Weapons of mass destruction, traditional terrorism, cyber terrorism, environmental change, the rise of regional hegemony, and the ascendancy of non-state actors (e.g. transnational criminal organizations) may all challenge US interests. Additionally, demographic trends, particularly increasing population and urbanization, are likely to exacerbate domestic and international tensions.

Although the U.S. is currently the lone superpower, it is unlikely to remain so indefinitely. Even without a peer competitor, niche competitors or aspiring regional hegemony may challenge U.S. interests and national security. Even where they do not directly threaten the United States, they may threaten global economic stability, which is a vital national interest. As the world moves towards a truly global economy, insulating the United States from economic turmoil will be more difficult. Therefore, isolationism as an option for national security strategy is both unattractive (except to a minority) and impractical. Consequently, the United States will remain "engaged." However, the scope of engagement and the means to achieve and sustain it are the subjects of ongoing debate.

It is also highly unlikely that these niche competitors and regional hegemons will confront the U.S. on the conventional battlefield. Rather, they will continue to search for asymmetric strategies, including IO and WMD, to achieve their goals/objectives. Conventional forces are not organized, trained, nor equipped to deal with these threats. Economic and political constraints further limit the utility of conventional forces to respond to these threats. Given these realities, it is likely that there will be continued demand for SOF.

Yet, SOF must also deal with limited resources in the face of growing commitments. The opportunities provided by the Revolution in Military Affairs may offer a solution to this dilemma. This RMA is characterized by application of information technology to enable innovations that fundamentally alter the conduct of military operations; it is an attempt to leverage technological superiority into strategic superiority. One aspect of this RMA is the emerging field of Information Operations, which seeks to capitalize on the growing dependency on information technology. IO offers a potential solution to dilemma of limited resources and growing commitments.

Chapter II discussed concepts of Information Operations. Because IO is an immature discipline, there are disputes over terminology and scope. The term "information operations" was adopted instead of "information warfare," which is too restrictive. "Warfare" connotes open, armed conflict and leaves out operations conducted during peacetime and conflict short of war. Information can be exploited for strategic advantage during peace, conflict or war by a variety of actors, not just the military. This

convention recognizes that the strategic utility of information is not limited to the battlefield.

The digitization of the battlefield and other attempts to strengthen our own C4I were excluded from the realm of IO. This is not because they lack benefit, but because they view information as an enabler of traditional combat rather than a separate realm of conflict. Additionally, including *every* application of information technology under the rubric of information operations renders the concept so broad as to be meaningless.

The sections that followed identified, described, and contrasted the two primary concepts of IO: the infrastructure approach and the psychological approach. Both approaches seek to exploit an adversary's dependence on information, but each has a different focus. The infrastructure approach targets the information systems and processes of an adversary and employs denial of service attacks on these targets. This approach appears to be the dominant perspective within the Department of Defense. The focus is on destroying or disrupting the systems in order to take away the adversary's means to react, resist, or maintain societal order. The goal is to cripple information dependent systems, reducing the ability of adversary to respond effectively; the adversary will have few options other than to consent to the attackers' demands. Denial of service attacks can be accomplished through a variety of means including physical destruction, directed energy weapons, malicious software, and other forms of computer network attack.

The psychological approach focuses primarily on the subtle manipulation of the decision-making processes of an adversary. Unlike the technological approach, which the DoD has publicly embraced, this particular psychological approach has not been officially

declared a part of information operations. This approach adapts and integrates the traditional disciplines of psychological operations, deception, and propaganda to information technologies to manipulate the understanding and perceptions of adversary. In contrast to the infrastructure attacks, this approach does not regularly seek to deny service. Rather, it seeks to insert or alter information without destroying the system. The immediate goal is influencing, or possibly even controlling, the adversary by managing or manipulating perceptions. The ultimate goal is to cause the adversary to make decisions and act upon them in ways that will support friendly strategic objectives. Advances in information technology allow more selective targeting than traditional techniques of persuasion.

The United States' growing dependency on information technology applications demands a defensive IO capability. Although this is important, the role of SOF in this endeavor will be principally limited to offensive tactical operations in support of a strategic defensive. SOF are primarily designed to carry out offensive operations; because of their limited numbers, they are not well suited to defensive operations. Additionally, unlike traditional defense, the responsibility for defending against IO will fall on other government agencies and domestic law enforcement.

Chapter III addressed the strategic integration of SOF and IO with SOF in a supporting role. It identified three core competencies (access, regional orientation, and adaptability) and the strategic utility of SOF, which results from employing these competencies. The strategic utility of SOF has several facets: expanded options, economy

of force, and tailor to task capabilities. Applying this utility in support of IO increases the scope of strategic IO while providing a strategic economy of force.

The core competencies of SOF are well suited to conducting or enhancing IO. SOF have the ability to operate in remote, denied or politically sensitive regions of the world that conventional forces cannot access. The ability to gain access to remote or denied areas is highly useful for the infrastructure approach to IO. This competency is enhanced by regional orientation of SOF. The language and cultural skills of SOF allow them to operate in areas where conventional forces may be unwelcome. They also provide SOF with an understanding of a region that can provide support for a psychological approach to IO. Additionally, the employment of SOF can itself influence the political will and commitment of both allies and adversaries. Finally, the maturity and experience of SOF operators, a willingness to try unconventional approaches and a flexible command and control structure, provide SOF with unrivaled adaptability. As the field of IO matures, SOF are well suited for developing and implementing innovative solutions to technical, tactical or organizational problems.

Chapter IV examined the integration of SOF and IO with IO in a supporting role, enhancing the ability of SOF to execute tactical missions. For short duration special operations, the concepts of a decision cycle (the OODA loop) and of relative superiority provided a framework for this examination. The concept of relative superiority was expanded from its original form to include the entire operation, from initial planning to successful exfiltration. IO provides a variety of means to disrupt the adversary's decision cycle at various points in order to achieve, extend, or sustain relative superiority. Both the

psychological and infrastructure approaches to IO offered proved beneficial in this regard. By slowing the relative speed of the enemy's decision cycle, IO can allow SOF to operate with the initiative and achieve or sustain relative superiority. Even when the enemy has well prepared defenses and contingency plans, IO can frustrate their implementation. This may provide the crucial time and space for SOF to achieve their mission.

Chapter IV also assessed the ability of IO to support protracted special operations, and found numerous applications. Extended duration special operations may include UW, FID, CA and collateral activities such as humanitarian assistance or peace operations. Admiral J.C. Wylie's concepts of sequential and cumulative strategies provided a framework for this assessment. While short duration operations are well suited to a sequential IO strategy, extended-duration operations benefit from the use of a cumulative strategy. Although these strategies are not mutually exclusive, a cumulative strategy is more appropriate for extended duration operations. This is particularly true of the psychological approach to IO since perception and understanding usually develop over long periods.

Both approaches to IO are useful for supporting UW missions. Infrastructure attacks can facilitate insurgent combat actions in the same manner that they support unilateral SOF actions – by disrupting the enemy decision cycle. They are also useful for undermining confidence in the incumbent regime. Additionally, they can support insurgent propaganda efforts. All of these efforts can contribute to recruiting and can also help increase popular support.

A psychological approach to IO is useful for many of the collateral activities, particularly when the use of force is restricted. Further, a psychological approach to IO may be the best option for primary SOF missions and collateral activities where the infrastructure is non-existent or severely damaged. In humanitarian efforts, peace operations, and CA missions, IO can support efforts to establish control of the local population and to secure their cooperation. If SOF can successfully accomplish these tasks, the need for deployment of conventional forces may be reduced or eliminated altogether.

Chapter V examined the impact of the integration of SOF and IO on the roles and missions for SOF. Increased demand for SOF and constrained resources require a careful analysis of roles and missions, both old and new. The traditional roles of commando and unconventional warrior have been expanded; SOF now play the role of commando, regional engagement force, humanitarian and law enforcement support.

Accepting additional missions may jeopardize the ability to execute current missions. Conversely, failing to accept new missions and adapt to the environment threatens national security and the future viability of USSOCOM. Yet, SOF cannot simply discard existing missions; in many cases, the conventional forces are unwilling or unable to accept them. Four criteria were proposed as the starting point for the evaluation of roles and missions:

- SOF core competencies should be essential to mission success
- A SOF mission should not duplicate capabilities resident in conventional forces.
- A new mission must not adversely affect the ability of SOF to execute current missions.

- The mission should contribute to realization of strategic objectives.

IO satisfies these criteria. First, it builds on existing core competencies and can support all of the existing roles that SOF play in the national security strategy. Chapter III discussed how SOF core competencies contributed to specific IO missions. With respect to the infrastructure approach, SOF core competencies were essential for infrastructure attacks and certain types of special reconnaissance in isolated or denied areas. Second, the capabilities that SOF bring to IO are not duplicated in the conventional force. Third, although the potential always exists, there is no *prima facie* reason that accepting IO should compromise the ability of SOF to execute other assigned missions. To the contrary, a robust IO capability should enhance the ability of SOF to execute these other missions. Fourth, it is a well-established fact that SOF, when properly employed, can have considerable strategic effect; properly integrating SOF and IO enhances the strategic utility of both SOF and IO.

Adopting IO as a principal mission will pose new challenges for SOF, particularly in the area of doctrine, training, recruiting, and materiel acquisition. USSOCOM is well suited to tackle these challenges. Recall that Chapter III identified adaptability as a core competence of SOF. Organizational flexibility, mature and experienced personnel, and a willingness to try unconventional approaches to problems all contribute to this ability. The relative independence of USSOCOM, provided by separate funding of SOF activities and RD&A, also contributes to this adaptability. Adopting IO presents an opportunity to recognize and adapt quickly to emerging requirements. Adopting and integrating IO as a

principal SOF mission is a means to ensure continued relevancy without threatening the ability to execute current missions.

B. ISSUES OF INTEGRATION

1. Characteristics of Integrated SOF/IO

Identifying the ways in which SOF and IO can be integrated is only the first step toward integration. Achieving actual integration and reaping its benefits are far more difficult tasks. While identifying all of the steps necessary to achieve full integration is highly complex and beyond the scope of this thesis, the characteristics of integrated SOF and IO are more readily identified. Long-range planning, interagency coordination, and unity of effort, and realistic appraisals of the capabilities and limitations of both SOF and IO will characterize a full integration of SOF and IO.

As noted in Chapter V, IO will not be the exclusive domain of SOF, or any other single organization. Regardless of which IO concept is eventually adopted or emphasized, IO will involve a variety of players. Close interagency coordination is a pre-requisite for unity of effort. All players in the effort must share a unified plan of action in order to prevent "IO fratricide." This can occur when conflicting messages are directed at the same target audience by different organizations, undermining the efforts of all parties. A single player going "off message" may disrupt the entire plan. It may also occur when infrastructure attacks disrupt an information pathway that is being used by another organization to achieve psychological objectives, undermining the efforts of another agency. For example, if an intelligence agency is inserting corrupted data in a command

and control system to deceive an adversary, an effort to disable that system will undermine this effort. Given the size of the federal government and the increasing number of pathways for information to reach the target audience this is an essential task.

Interagency coordination can foster a unity of effort, which is necessary to avoid not only operational conflicts but also disputes over responsibilities and priorities. Like the issue of roles and missions in the Department of Defense, the issues of responsibility and authority for IO within the entire government is a contentious issue. For example, what agency or organization is responsible for ensuring adequate defensive measures? What are our defensive priorities for IO? Is it more important to stop an intrusion in progress or allow it to progress in order to determine the identity of an intruder? These and a host of other questions require answers; this task is made easier when all parties are working together toward common objectives.

Close coordination will also ensure careful consideration of the psychological and political implications of all SOF actions. Under ideal conditions, SO would not only achieve the desired physical effects but also psychological effects. Because of the political sensitivities surrounding many SOF missions, where failure can damage national prestige, close coordination at the interagency level between SOF and U.S. government agencies is absolutely necessary. In addition to reducing political risk, interagency coordination maximizes SOF effectiveness by ensuring that all available resources are employed.

Long-range planning is also important because of the detailed intelligence requirements for infrastructure attacks and the difficulty of changing perceptions with

single events. Both approaches to IO require detailed knowledge and understanding of the target, which is difficult to achieve on short notice. Therefore, it is incumbent upon all participants to plan and identify the intelligence required to support or implement the plan.

Long-range planning and close coordination also facilitates a realistic understanding of the capabilities and limitations of SOF. A thorough understanding of SOF capabilities and reasonable expectations can help prevent misuse, which can lead to tactical and strategic failure. Although SOF frequently works closely with some government agencies, not all of these agencies will have an understanding of how SOF can be enhance or enable IO. As they work more closely together over an extended period, both sides should become more familiar with the SOF capabilities.

2. Obstacles to integration

While the integration of SOF and IO has the potential to provide the United states a strategic advantage, it should not be a considered a “done deal.” Bureaucratic politics, both within DoD and among other government agencies, may present a significant obstacle to full integration. As noted earlier, there are and will continue to be “turf battles” concerning every aspect of IO, including its definition and scope. Additionally, SOF will continue to compete with the services for resources, roles, and missions. These types of battles may slow or prevent full integration if organizational self-preservation takes precedence over efficiency and mission accomplishment.

Another obstacle to full integration is the adoption of a narrowly defined or limited view of IO, principally the infrastructure approach. A narrow definition of IO that

focuses on computer network attack or forms of electronic warfare will exclude a variety of organizations from IO. This could create the same types of “stovepipes,” both intelligence and operational, that have been the hallmark of the Cold war era and it would limit the application of IO. A narrow scope of IO also increases the incentives for organizations with an existing stake to protect their interests rather than cooperating with other organizations. Although SOF would still have some role in this, it would likely be very limited. The next section examines in greater detail the reasons why a broader approach to IO is more appropriate as a basis for strategy.

C. ISSUES OF STRATEGY

Although this thesis is primarily concerned with the integration of SOF and IO, the result of this integration should support efforts to achieve strategic objectives. Therefore, it is appropriate to examine how integration supports the National Security Strategy (NSS) and National Military Strategy (NMS). How do the concepts support the NSS and the NMS? Which concept of IO should we use?

The implicit objectives of any national security strategy are the preservation of peace and protection of vital national interests. The United States has adopted a strategy of engagement and enlargement to achieve these goals and thereby ensure the nation’s security. The current National Security Strategy declares “First, we must be prepared and willing to use all appropriate instruments of national power to *influence* the actions of other states and non-state actors”(emphasis added).¹ An essential element if the National

¹ United States, *A National Security Strategy for A New Century* (Washington, D.C.: GPO, 1997) n.pag. Online. Internet. Available: www.whitehouse.gov/WH/EOP/NSC/Strategy

Military Strategy (NMS) that supports this goal is the objective of *shaping the international environment*. The NMS states:

The shaping element of our strategy helps foster the institutions and international relationships that constitute a peaceful strategic environment by promoting stability; preventing and reducing conflict and threats; and deterring aggression and coercion.²

While this goal is represents the ideal situation, the NMS recognizes that it may not always be possible to achieve it. Therefore, it also calls on the Armed Forces to be prepared to “*respond to the full spectrum of crises*” and “*prepare now for an uncertain future*.” While the psychological approach to IO can support each of these objectives, the infrastructure approach, by itself, offers very little limited support for shaping, which is arguably the most important element of the strategy; it is the essence of military support for the NSS. However, it can provide support to the psychological strategy, which is ideally suited for supporting engagement. This indicates that the psychological approach to IO is a more appropriate concept for supporting the NSS.

Table 6-1: IO Support for the National Military Strategy

	Infrastructure Approach	Psychological Approach
Shape	NO	YES
Respond	YES	YES
Prepare	YES	YES

² Dept. of Defense (The Joint Chiefs of Staff), *National Military Strategy: Shape, Respond, Prepare Now A Military Strategy for a New Era* (Washington D.C., 1997) n.pag. Online. Internet. Available: www.dtic.mil/jcs/nms/index.html

1. IO and Deterrence

Colin Gray believes that nothing is inherently deterring. Deterrence is a "cooperative" endeavor that works through "contingent explicit or implicit menaces."³ "Deterrence works when a person, organization, or state decides not to take a particular course of action because the net consequences are *judged* unduly negative." (emphasis added).⁴ Fred Walker asserts that this is a "clearly psychological phenomenon because it occurs in the mind of a potential enemy."⁵ Deterrence depends not only on an imbalance in capabilities but also in will and "when a conflict involves interests absolutely vital to an adversary but peripheral to the United States, an opponent may not yield short of a complete American victory in battle."⁶

In theory, the offensive nature of the infrastructure approach is well suited as a means of deterring potential adversaries. Whether the deterrence is based on the possibility of punishment or the prospect of denial, infrastructure attacks could contribute significantly. Deterrence by *denial* presents an adversary with the prospect that his forces will be defeated in the field and his objectives will thereby be denied.⁷ Infrastructure attacks could significantly degrade the command and control capabilities of an adversary and increase the vulnerability of his forces. In addition to degrading command and

³ Gray 32.

⁴ Gray 32.

⁵ Goldstein 18.

⁶ Nye and Owens 25.

⁷ Gray 33. See also John J. Mearsheimer, *Conventional Deterrence* (Ithaca: Cornell University Press, 1983) and Patrick M. Morgan, *Deterrence: A Conceptual Analysis* (Beverly Hills, Sage Publications, 1977).

control, these attacks could also undermine the supporting infrastructure, (e.g. the transportation systems or industrial production facilities.) and make it difficult to sustain military operations. When combined with the overwhelming U.S. advantage in conventional forces, these actions may deter a potential adversary. It is important to emphasize that achieving deterrence by denial requires a credible conventional threat as a complement. Even if an adversary's command and control or support infrastructure is significantly degraded, there is no guarantee that the United States would achieve its strategic objectives without the use of some type of conventional force. In the absence of this threat, infrastructure attacks will pose a significant threat but not a fatal blow an adversary.

Deterrence by *punishment* works by threatening the adversary with unacceptable penalties for his actions.⁸ The potential of infrastructure attacks to wreak havoc on the normal functioning of a society may be severe enough to deter a potential adversary. As noted earlier though, the efficacy of this approach is contingent on the adversary's reliance on information systems.

While information infrastructure attacks have great potential in theory, they currently have little value as a general deterrent for several reasons. First, despite the low entry cost of acquiring an infrastructure attack capability, the cost of developing the necessary intelligence could be much more costly. Any actor, including the United States, that wishes to carry out large-scale, coordinated attacks against the information infrastructure of an adversary requires a great deal of detailed intelligence.

Second, while the theoretical consequences of infrastructure attacks may be troubling, no nation or actor has demonstrated a capability to carry out large-scale attacks. There is a general reluctance on the part of most nations to even admit to a capability, much less a willingness, to carry out infrastructure attacks. Because of this reluctance, the effectiveness of these attacks is unproven and they lack credibility. Consequently, the capability to actually achieve the desired effect on the ultimate target, the decision-making or war making capability of the adversary, is also unproven. Of course, smaller, random attacks can inconvenience and obstruct an adversary but it is far from clear that they will constitute a significant threat. Referring back to Mahan, these attacks cause "great individual injury and discontent" but they are not, of themselves, capable of winning a war.

Third, not only is the capability unproven but it may be fleeting. The pace of technology evolution may undermine the durability of the methods utilized; some methods may only work once; other methods may become obsolete before they are ever applied. It is difficult to base a strategy of deterrence on a threat that may be rendered obsolete at any moment by simple security measures or improved technology. In the future, a robust infrastructure attack capability (based on computer network attack) may become, under certain circumstances, an effective component of a deterrence strategy

Fourth, many developing nations may not be as adversely affected by infrastructure attacks as the United States; it is difficult to gain leverage and influence by threatening something upon which an adversary does not depend. This is also true for

⁸ Gray 33.

non-state actors; they may be mobile and not rely on any particular information infrastructure. True, disabling the infrastructure of the host nation may temporarily disrupt the operations of a non-state adversary but it is unlikely to permanently cripple their organization. Additionally, targeting the information infrastructure of the host with anything other than pinpoint precision is likely to cause collateral damage to both the host and U.S. foreign relations.

Fifth, infrastructure attacks may also provoke a backlash in the international community and open a Pandora's Box of legal and ethical problems; domestic opposition may be high also. The United States is highly dependent on advanced information systems and highly vulnerable and would likely suffer considerably if other nations adopted this approach. Additionally, the use of infrastructure attacks in any situation outside of a declared war may actually lead to a conventional confrontation if it is unsuccessful, or infrastructure counterstrikes against the US by the target nation's allies or proxies. It is also possible that other adversaries may respond to these attacks with WMD or terrorist attacks. Recall that Russia has publicly discussed adopting a policy of responding to infrastructure attacks with nuclear weapons.⁹

Adopting an infrastructure approach as the basis of a strategy has other problems as well. It relies on the nebulous concepts of "information dominance" or "information superiority." There is an ongoing debate over the validity and value of the concepts of "information superiority" and "information dominance," particularly because the concepts

⁹ Timothy L. Thomas, "Russian Views on Information-Based Warfare," *Air Power Journal* July 1996 Special Edition: 26.

are difficult to quantify. How would we know when we had achieved either? What are the measures of effectiveness? How can we be sure, except after the battle, that we had truly achieved it? How do we know if we have lost it? It is entirely possible that an adversary will effectively portray an image of having lost the ability to effectively gather and use information. The adversary may allow this to occur because he actually has a better *understanding* of the situation.

The fact that one side possesses information does not prevent the use of information by the other side. Secondly, some information is more valuable than other information; it is not simply a matter of having more information. The balance could conceivably be tipped by a very small, seemingly inconsequential, piece of data. Strategy, operations, and tactics will define the information needs of each side in a conflict; what is valuable to one party may be useless to the other. Libicki points to the case of Somalia: "The United States enjoyed information superiority at the tactical level—its forces could see objects from great distances. But, its insight at the operational level and the political level was inferior to what its adversaries enjoyed." Poor strategy can rarely be saved by tactical information superiority.¹⁰

In summary, the infrastructure approach is not appropriate as a basis of strategic policy that seeks to deter. It does not address how targeting "information and information systems" effectively influences decision-makers without first resorting to actions that may

¹⁰ Martin Libicki, "Information Dominance" *INSS Strategic Forum* Number 132, November 1997. n.pag. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum

be considered acts of war. Nor does it allow for influencing less developed nations that do not depend on information systems.

2. IO Concepts and the Analogy to Sea Power

Although imperfect, the analogy between information (as a medium) and the sea is useful for thinking about how these IO concepts relate to strategy.¹¹ Like the oceans, the information realm spans the globe and is an essentially neutral medium, which is not owned by any single state. Similarly, ideas and the means to communicate them are not owned by any particular state (although some states attempt to monopolize information within their borders). This analogy is particularly appropriate for the Internet but applies to other communications mediums as well.

The sea power strategies described and analyzed by Mahan, sea denial and sea control, parallel the concepts of IO identified in the preceding sections. The infrastructure approach to IO can be compared to Mahan's sea denial strategy. Sea denial, or "commerce-destroying" as Mahan called it, involves denying an adversary use of the sea.¹² It can provide a means to slow his response, cause "great individual injury and discontent," or avoid losing a war but is not a means to winning a war. Infrastructure attacks perform a similar function. They deny an adversary the use of an information

¹¹ Buddenberg, Rex, "The Network and Doctrine." Unpublished class notes. Naval Postgraduate School, 1997.

¹² Alfred T. Mahan, *The Influence of Sea Power on History: 1600-1783*, (New York: Dover Publications Inc., 1987). For a discussion of the modern applications of Mahan's theories see John Sumida Tetsuro, *Inventing Grand Strategy and Teaching Command: The Classic Works of Alfred Thayer Mahan Reconsidered*, Baltimore: Johns Hopkins University Press, 1997.

medium. Denial of service attacks may also generate “great individual injury and discontent” but they are not, of themselves, capable of winning a war.

For Mahan, sea control meant the ability to transport men and materiel to distant regions in order to project forces; it facilitated success in land based operations. At the same time, it required limiting the sea denial capabilities of the enemy. Control provides the freedom to attack as well as freedom from attack. Achieving control of the sea also required a significantly larger investment than maintaining a sea denial capability. The psychological approach to IO is analogous to this; a strategy based on this approach requires the ability to project information and ideas to influence an adversary. Shaping perceptions requires exercising a significant degree of control over the information available to the target audience. At the same time, it requires taking steps to ensure that your adversary cannot limit or disrupt your use of a particular medium. Like sea control, achieving control of the information realm requires significantly more resources but it can enable the application of other elements of national power. It may even reduce the need for the application of force.

Like Mahan’s strategies, the concepts of IO identified here are not mutually exclusive. Rather, they are complementary and mutually supporting. Like sea power (and air power), information “power” cannot win wars unilaterally. However, the application of sea power and information power can, under certain circumstances, deter adversaries and prevent conflicts. It is therefore useful to examine the deterrence capabilities of the different approaches to IO.

3. Strategic Emphasis

The two concepts of IO described in this thesis are not antithetical but complementary. Although the psychological approach is more appropriate to an overarching IO strategy, the infrastructure approach can and should be a component of this strategy. It can support the psychological approach by providing the means to penetrate information systems and manipulate the information to convey the desired message. It can also be applied destructively in more limited circumstances, e.g. to prevent an imminent conflict or gain an advantage in one that has already begun by "blinding" the command and control functions of an adversary.

An important distinction needs to be emphasized regarding the use of information infrastructures in the two conceptual approaches. While both can exploit an adversary's dependence on information technology, the results and objectives are quite different. For the infrastructure approach, the goal is to cripple information dependent activities by disrupting or destroying the information systems. Although the perpetrators may remain anonymous, the failure or destruction will be obvious. Conversely, the psychological approach attempts to manipulate perceptions and understanding by penetrating the information systems in order to control the information flowing through them. If carried out properly, this penetration should remain undetected by the target.

There are several reasons why a psychological strategy is more appropriate. First, as noted above it provides the basis for a strategy applicable across the entire spectrum of conflict. While many military activities are reactionary in nature, a psychological approach can (and should) be employed on a continuous basis. The means utilized in

this approach do not necessarily involve the use of force or actions that could reasonably be construed as 'force.' Therefore, it has the potential to provide not only conflict prevention but also peaceful conflict resolution. On the other hand, attacking the infrastructure of an adversary could possibly be construed as an act of war.¹³ It is difficult to reconcile an infrastructure approach with a strategy of peacetime engagement.

Secondly, it allows for the utilization of the United States immense communications capabilities, both in government and in the private sector, to influence the perceptions and behavior of foreign audiences. No other nation can match the communications resources at the disposal of the United States. As Admiral William Owens and Joseph Nye write:

This new political and technological landscape is ready-made for the United States to capitalize on its formidable tools of soft power, to project the appeal of its ideals, ideology, culture, economic model, and social and political institutions, and to take advantage of its international business and telecommunications networks.¹⁴

Finally, although this approach can exploit advances in technology, it is not dependent on technology. Although the medium used to communicate a desired message may vary, developed and developing nations are each susceptible to a well-conceived and orchestrated psychological strategy.

¹³ For a detailed discussion see Lawrence T Greenberg, Seymour E. Goodman and Kevin J. Soo Hoo. *Information Warfare and International Law* (Carlisle Barracks: National Defense University Press, 1998) Online. Internet. Available: www.DoDccrp.org/iwilindex.htm

¹⁴ Joseph S Nye, Jr. and William A. Owens. "America's Information Edge" *Foreign Affairs* March April 1996: 29.

While some advocates of IO have promoted it as a possible alternative to armed conflict and bloodshed, this is impractical and runs counter to history. Nevertheless, to further the objectives of the NSS, the concept of IO adopted should provide an ability to influence adversaries that reduces both the necessity and probability of armed conflict. Therefore, this concept should attempt to reduce our dependence upon physical destruction. In short, to achieve its full potential, IO should focus on influencing decision-makers; the psychological approach does this in a more direct way and is applicable across the entire spectrum of conflict. The infrastructure approach attempts to influence the decision-makers indirectly by crippling the adversary's capabilities. While useful, it is better suited as a component of the psychological strategy and a holistic view of IO allows for both approaches.

In summary, the United States and USSCOM should adopt an IO strategy predicated on achieving psychological influence using all instruments of information power. Not only does this approach better support the NSS but it also maximizes the utility of integrated SOF and IO. As previously noted, IO will not be the province of any single organization or agency; it requires a disciplined inter-agency approach. SOF needs support from the other government agencies and military organizations - support that will not be forthcoming unless they all share a similar concept of IO - even though some organizations may focus on different aspects of IO. A definition of IO based on this concept would therefore focus on achieving that goal. A proposed definition for IO would be similar to the current definition of psychological operations:

Actions to influence the understanding, perception, and objective reasoning of foreign decision-makers at all levels by conveying and/or denying selected information and indicators.

Unlike the current DoD definition, this definition does not focus on “adversary information and information systems” but rather on the functions that are dependent upon information. It is through this influence that the United States is most likely to achieve its strategic goals without having to resort to the expensive and politically risky commitment of conventional forces.

Under this definition, there is no discrete set of operations that can be labeled “information operations.” More than anything else, it is a paradigm shift. Although this phrase is overused, it is irreplaceable in this context. The psychological impact of every action must be considered; they must be viewed from the perspective of our adversary and avoid mirror imaging. This approach also requires a cumulative strategy to achieve its full potential.

Although there is still some confusion in DoD, some sectors are beginning to realize the true strategic value of IO as a tool of influence. The following passage is excerpted from the Joint Staff publication *Concept for Future Joint Operations*:

The effectiveness of deterrence, power projection, and other strategic concepts is greatly affected by the ability of the US to *influence the perceptions and decisions of others*. In times of crisis, IO can help deter adversaries from initiating actions detrimental to the interests of the US, its allies, or the conduct of friendly military operations. If carefully conceived, coordinated, and executed, IO can make an important contribution to defusing a crisis; reducing the period of confrontation; enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ forces in combat. (emphasis added)¹⁵

In order to achieve the desired level of influence any strategy adopted must integrate and coordinate the multitude of government agencies involved. This strategy would also require a commitment to continuous application, a 365-day-a-year approach. This is not an easy task; it will require overcoming bureaucratic barriers to cooperation and instilling a new mindset regarding IO. Instilling a new mindset requires removing IO from the realm of futurists and fiction and avoiding what Martin Libicki calls "hammer madness":

There is a tendency, which one can call "hammer madness." "Hammer madness" comes from the phrase, "If all you own is a hammer, then the entire world begins to look like a nail." If you have a high-tech information-rich war-fighting machine, you will have its natural tendency to take a look at military operations as things that can be done by this high-tech information warfare machine. Well, a lot of things can be done by this machine. That machine is a glorious thing for doing certain operations, but on the other hand, it is not appropriate for screws. It's not appropriate for many of the low-technology wars that we may get into. It's not necessarily going to be appropriate for peace operations. It's not necessarily going to be appropriate for psychological warfare.¹⁶

¹⁵ Dept. of Defense, *Concept for Future Joint Operations: Expanding Joint Vision 2020* (Washington, D.C.: Dept. of Defense (JCS), May 1997) 42.

¹⁶ *Approaching the Digital Battlefield*, Transcript, "America's Defense Monitor" Center For Defense Information, Washington, D.C., 15 Dec 1996.

While technology is important, it is not the essence of the psychological approach nor should it be the foundation of an IO strategy.

D. CONCLUSION

Special Operations Forces (SOF) have assumed a unique and expanded role as a strategic asset of the United States. The conjunction of a changing political and security environment and new technologies present both challenges and opportunities for SOF. Special Operations Forces provide the National Command Authority (NCA) a variety of unique capabilities and expanded options for achieving strategic goals with minimum costs. The recent drawdown has placed even more value on the capabilities and leverage provided by SOF. Additionally the rapid pace of technological change – the “information revolution” – has opened the door to a potential “Revolution in Military Affairs” (RMA). New approaches to “warfare” like Information Operations (IO) are beginning to emerge from the RMA. Information operations, like SOF, can also provide a means to leverage limited resources. In general terms, there are two general categories: IO in support of special operations (SO), and SO in support of IO. Each has distinct implications for SOF. In either case, the object of the supporting operation is to generate or expand a window of opportunity for the supported operation. Separately, both SO and IO can provide economy of force. Properly employed, this leverage is multiplied and offers a tremendous strategic asset.

E. RECOMMENDATIONS FOR FUTURE RESEARCH

A particularly valuable avenue for future research is the application of these concepts to different scenarios to evaluate their impact more fully. This research would be invaluable in determining the specific doctrinal, organizational, operational, and materiel solutions necessary to fully integrate SOF and IO. There are a number of detailed scenarios currently available that could provide the basis for this research. For example, the US Air Force study, *AF 2025*, provides six detailed scenarios set in 2025. This research should also include coordination with the USSOCOM Future Concepts Working Group to provide input for the long range planning process.

APPENDIX A. GLOSSARY OF DoD DEFINITIONS

Unless otherwise noted, the following definitions are from Joint Publication 1-02, *DoD Dictionary of Military and Associated Terms* (available at <http://www.dtic.mil/doctrine/jel/>).

Air Superiority : That degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force.

Air Supremacy: That degree of air superiority wherein the opposing air force is incapable of effective interference.

Black propaganda: Propaganda which purports to emanate from a source other than the true one.

Clandestine operation: An operation sponsored or conducted by governmental departments or agencies in such a way as to assure secrecy or concealment. A clandestine operation differs from a covert operation in that emphasis is placed on concealment of the operation rather than on concealment of identity of sponsor. In special operations, an activity may be both covert and clandestine and may focus equally on operational considerations and intelligence-related activities. See also covert operation; overt operation.

Command and control: The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of

personnel, equipment, communications, facilities, and procedures employed by a Commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2.

Command and control system: The facilities, equipment, communications, procedures, and personnel essential to a commander for planning, directing, and controlling operations of assigned forces pursuant to the missions assigned.

Command and control warfare: 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. Command and control warfare is an application of information warfare in military operations and is a subset of information warfare. Command and control warfare applies across the range of military operations and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. C2-attack. Prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protect. Maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control; electronic warfare; intelligence; military deception; operations security; psychological operations.

Communications Security: (DOD) The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from

the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. Also called COMSEC. Communications security includes: cryptosecurity, transmission security, emission security, and physical security of communications security materials and information. a. Cryptosecurity –The component of communications security that results from the provision of technically sound cryptosystems and their proper use. b. Transmission security –The component of communications security that results from all measures designed to protect transmissions from interception and exploitation by means other than cryptanalysis. c. Emission security –The component of communications security that results from all measures taken to deny unauthorized persons information of value that might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems. d. Physical security –The component of communications security that results from all physical measures necessary to safeguard classified equipment, material, and documents from access thereto or observation thereof by unauthorized persons.

Computer Security: The protection resulting from all measures to deny unauthorized access and exploitation of friendly computer systems. Also called COMPUSEC. See also communications security.

Counterdeception: Efforts to negate, neutralize, diminish the effects of, or gain advantage from, a foreign deception operation. Counterdeception does not include the intelligence function of identifying foreign deception operations. See also deception.

Covert operation: An operation that is so planned and executed as to conceal the identity of or permit plausible denial by the sponsor. A covert operation differs from a clandestine operation in that emphasis is placed on concealment of identity of sponsor rather than on concealment of the operation. See also clandestine operation; overt operation.

Critical information: Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment.

Critical node: An element, position, or communications entity whose disruption or destruction immediately degrades the ability of a force to command, control, or effectively conduct combat operations.

Cryptology: The science which deals with hidden, disguised, or encrypted communications. It includes communications security and communications intelligence.

Data: Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned.

Deception: Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. See also counterdeception; military deception.

Directed-energy warfare: Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of

enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. See also directed energy; directed-energy device; directed-energy weapon; electromagnetic spectrum; electronic warfare.

Dominant Battlespace Knowledge: Comprehensive awareness of all the decision-relevant elements within a defined battlespace, and the ability to predict, with very high confidence, near-term enemy actions and combat outcomes.¹

Electromagnetic intrusion: The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. See also electronic warfare."

Electronic warfare: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack. That division of electronic warfare involving the use of electromagnetic, directed energy, or anti-radiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic

spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection. That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support. That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence, both communications intelligence, and electronics intelligence. See also command and control warfare; communications intelligence; directed energy; directed-energy device; directed-energy warfare; directed-energy weapon; electromagnetic compatibility; electromagnetic deception; electromagnetic hardening; electromagnetic jamming; electromagnetic spectrum; electronics intelligence; frequency deconfliction; signals intelligence; spectrum management; suppression of enemy air defenses.

¹ National Security Agency, *National Cryptologic Strategy for the 21st Century* (Washington, D.C.: GPO, 1997) n.pag. Online. Internet. Available: www.nsa.gov:8080/programs/ncs21

Global information infrastructure: The worldwide sum of all interconnected information systems and the systems that connect them. Also called GII. See also information; information system.

Grey propaganda: Propaganda that does not specifically identify any source.

Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation.

Information Assurance: Information operations that protect and defend information and 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. Also called IA. (DoD, *Joint Publication 3-13, Joint Doctrine for Information Operations* (Final Draft)).

Information dominance: The degree of information superiority that allows the possessor to use information systems and capabilities to achieve an operational advantage in a conflict or to control the situation in operations other than war while denying those capabilities to the adversary. (Dept. of the Army, *FM 100-6 Information Operations*).

Information infrastructure: Linkages of individual information systems in a myriad of direct and indirect paths that transcend industry, media and the military and include both government and non-government entities. Human collection, processing, and dissemination of information is an integral part of the information infrastructure. Includes 3 categories: global information infrastructure (GII), national information infrastructure

(NII), and defense information infrastructure (DII). (*Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare*, 1995)

Information superiority: That degree of dominance in the information domain which permits the conduct of operations without effective opposition.

Information warfare: (1) Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW. (2) Information operations conducted during the time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (From Joint Publication 3-13, *Joint Doctrine for Information Operations* (Final Draft))

Information system: The organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. In information warfare, this includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, disseminate, and act on information. See also information; information warfare.

Military deception: (DOD) Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions)(sic) that will contribute to the accomplishment of the friendly mission. The five categories of military deception are: a. strategic military deception—Military deception planned and executed by and in support of senior military commanders to result in adversary military policies and

actions that support the originator's strategic military objectives, policies, and operations.

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

Operations security: A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to

adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. See also command and control warfare; operations security indicators; operations security measures; operations security planning guidance; operations security vulnerability.

Overt peacetime psychological operations programs: Those programs developed by combatant commands, in coordination with the chiefs of US diplomatic missions, that plan, support, and provide for the conduct, during military operations other than war, of psychological operations in support of US regional objectives, policies, interests, and theater military missions. Also called OP3. See also consolidation psychological operations; psychological operations.

Perception management: Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. See also psychological operations.

Preemptive attack: An attack initiated on the basis of incontrovertible evidence that an enemy attack is imminent.

Preventive war: A war initiated in the belief that military conflict, while not imminent, is inevitable, and that to delay would involve greater risk.

Propaganda: Any form of communication in support of national objectives designed to influence the opinions, emotions, attitudes, or behavior of any group in order to benefit the sponsor, either directly or indirectly. See also black propaganda; gray propaganda; white propaganda.

Psychological consolidation activities: Planned psychological activities in peace and war directed at the civilian population located in areas under friendly control in order to achieve a desired behavior which supports the military objectives and the operational freedom of the supported commanders.

Psychological operations: Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. See also consolidation psychological operations; overt peacetime psychological operations programs; perception management.

Psychological warfare: The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives. Also called PSYWAR. See also psychological warfare consolidation.

Sea Control Operations: The employment of naval forces, supported by land and air forces, as appropriate, to achieve military objectives in vital sea areas. Such operations include destruction of enemy naval forces, suppression of enemy sea commerce,

protection of vital sea lanes, and establishment of local military superiority in areas of naval operations. See also land control operations.

Special Operations: 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. These operations are conducted across the full range of military operations, independently or in coordination with operations of conventional, non-special operations forces. Political-military considerations frequently shape special operations, requiring clandestine, covert, or low visibility techniques and oversight at the national level. Special operations differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets. Also called SO.

Special information operations: Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process. (From Joint Publication 3-13, *Joint Doctrine for Information Operations* (Final Draft)).

Strategic psychological activities: Planned psychological activities in peace and war which normally pursue objectives to gain the support and cooperation of friendly and neutral countries and to reduce the will and the capacity of hostile or potentially hostile countries to wage war.

Strategy: The art and science of developing and using political, economic, psychological, and military forces as necessary during peace and war, to afford the maximum support to policies, in order to increase the probabilities and favorable consequences of victory and to lessen the chances of defeat. See also military strategy; national strategy.

White propaganda: Propaganda disseminated and acknowledged by the sponsor or by an accredited agency thereof.

APPENDIX B. GLOSSARY OF COMPUTER SECURITY TERMS

This appendix contains a selection of computer security terms that are relevant to discussions of infrastructure attacks and penetration of computer networks. Unless accompanied by a specific citation, the definitions below were provide by the United States Air Force Computer Emergency Response Team (AFCERT) Computer Security Glossary , which can be found online at <http://afcert.csap.af.mil/term.html>.

Anomaly detection: "A label for the class of intrusion detection tactics which seek to identify potential intrusion attempts by virtue of their being (presumably) sufficiently deviant (i.e., 'anomalous') in comparison with expected / authorized activities. Phrased another way, anomaly detection begins with a positive model of expected system operations and flags potential intrusions on the basis of their deviation (as particular events or actions) from this presumed norm. Cf. misuse detection. "Anomaly detection techniques assume that all intrusive activities are necessarily anomalous. This means that if we could establish a "normal activity profile" and maintain a "current activity profile" for a system, we could, in theory, flag all system states varying from the established profile by statistically significant amounts as intrusion attempts." ¹

Application gateway: "One form of a firewall in which valid application-level data must be checked / confirmed before allowing a connection. In the case of an ftp

¹ Aurobindo Sundaram, "An Introduction to Intrusion Detection," *Crossroads* 1996: n.pag. Online. Internet. Available: www.acm.org/crossroads/xrds2-4/intrus.html

connection the application gateway appears as a ftp server to the client and as a ftp client to the server.” (AFCERT Computer Glossary)

Assurance: “A measure of confidence that the security features and architecture of an information system / network accurately reflect and enforce the given security policy.” (AFCERT)

Audit trail: “The chronological set of records that provides evidence of system activity. These records can be used to reconstruct, review, and examine transactions from inception to output of final results. The records can also be used to track system usage and detect and identify intruders.”²

Availability: “A security principle that ensures the ability of a system to keep working efficiently and to keep information accessible. Contrast with *denial of service*”.³

Also: “Computer hardware and software system working efficiently and the system is able to recover quickly and completely if a disaster occurs. The principle that ensures that computer systems and data are working and available to users. Denial of service is an attack on availability.” (AFCERT Computer Glossary)

Back Door: “A hole in the security of a computer system deliberately left in place by designers or maintainers. Synonymous with trap door; A hidden software or hardware mechanism used to circumvent security controls. A breach created intentionally for the purpose of collecting, altering or destroying data.” (AFCERT Computer Glossary)

² Deborah Russell and G.T. Gangemi Sr., *Computer Security Basics* (Cambridge: O'Reilly and Associates, 1992) 405.

³ Russell and Gangemi 405.

CERT: Computer Emergency Response Team

Confidentiality: "The principle that keeps information from being disclosed to anyone not authorized to access it. Synonymous with secrecy." (AFCERT Computer Glossary)

Countermeasures: "Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system. Countermeasures that are aimed at specific threats and vulnerabilities involve more active techniques as well as activities traditionally perceived as security." (AFCERT Computer Glossary)

Denial of service: "Action(s) which prevent any part of an AIS from functioning in accordance with its intended purpose. See Availability".

DNS spoofing: "A form of spoofing which exploits the Domain Name Service (DNS) by which networks map textual domain names onto the IP numbers by which they actually route data packets. "Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain." (AFCERT Computer Glossary)

Emanations: "Electrical and electromagnetic signals emitted from electrical equipment (e.g. computer, terminals, printers, cabling) and transmitted through the air or through conductors. If the information carried by these emanations is intercepted and deciphered, sensitive information may be compromised. Also called emissions".⁴

Firewall: "A system or combination of systems that enforces a boundary between two or more networks. Gateway that limits access between networks in accordance with

local security policy. The typical firewall is an inexpensive micro-based Unix box kept clean of critical data, with a bunch of modems and public network ports on it but just one carefully watched connection back to the rest of the cluster.” (AFCERT Computer Glossary)

Fishbowl: “A defensive IW tactic in which a suspicious or unauthorized user is permitted to continue established access to the protected system / network, but whose interactions with that system / network are (all unknown and unapparent to the subject) 'encapsulated' within a secure domain of operations (e.g., rerouted to an isolated computer; redirected to a dummy environment simulating an actual server) so that IW defenders can observe and analyze the user's intentions, tactics, and/or identity”.⁵

Also: “To contain, isolate and monitor an unauthorized user within a system in order to gain information about the user.” (AFCERT Computer Glossary)

Hacker: “A person who enjoys exploring the details of computers and how to stretch and test their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around. A person who enjoys learning the details of programming systems and how to stretch their capabilities, as opposed to most users who prefer to learn only the minimum necessary.” (AFCERT Computer Glossary)

Intrusion detection: “Pertaining to techniques which attempt to detect intrusion into a computer or network by observation of security logs or audit data. Detection of

⁴ Russell and Gangemi 411.

⁵ Randall Whitaker, *The Convolution Terminology of Information Warfare*. Online. Internet. Available: www.informatik.umu.se/~rwhit/IWGlossary.html

break-ins or attempts either manually or via software expert systems that operate on logs or other information available on the network.” (AFCERT Computer Glossary)

IP splicing / hijacking: “An attack whereby an active, established, session is intercepted and co-opted by the attacker. IP splicing attacks may occur after an authentication has been made, permitting the attacker to assume the role of an already authorized user. Primary protections against IP splicing rely on encryption at the session or network layer.” (AFCERT Computer Glossary)

IP spoofing: “An attack whereby a system attempts to illicitly impersonate another system by using IP network address.” (AFCERT Computer Glossary)

Keystroke monitoring: “A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the host computer returns to the user.” (AFCERT Computer Glossary)

Letter bomb: “Malicious / disruptive code delivered via an email message (and / or an attachment to said message). "A piece of email containing live data intended to do malicious things to the recipient's machine or terminal. Under UNIX, a letter bomb can also try to get part of its contents interpreted as a shell command to the mailer. The results of this could range from silly to tragic.” (AFCERT Computer Glossary)

Logic bomb: “A resident computer program which, when executed, checks for particular conditions or particular states of the system which, when satisfied, triggers the perpetration of an unauthorized act.” (AFCERT Computer Glossary)

Mockingbird: "A computer program or process which mimics the legitimate behavior of a normal system feature (or other apparently useful function) but performs malicious activities once invoked by the user." (AFCERT Computer Glossary)

Packet: "A generic term for protocol unit. The unit of data sent across a packet switching network. The term is used loosely. While some TCP/IP literature uses it to refer specifically to data sent across a physical network, other literature views an entire TCP/IP internet as a packet switching network and describes IP datagrams as packets." (AFCERT Computer Glossary)

Packet Sniffer: "A device or program that monitors the data traveling between computers on a network." (AFCERT Computer Glossary)

Packet sniffing: "Packet sniffing is a technique in which attackers surreptitiously insert a software program at remote network switches or host computers. The program monitors information packets as they are sent through networks and sends a copy of the information retrieved to the hacker. By picking up the first 125 keystrokes of a connection, attackers can learn passwords and user identifications, which, in turn, they can use to break into systems."⁶

Password sniffing: "Sniffers are programs that monitor all traffic on a network, collecting a certain number of bytes from the beginning of each session, usually the part where the password is typed unencrypted on certain common Internet services such as FTP and Telnet." (AFCERT Computer Glossary).

⁶ Whitaker n.pag.

Penetration: "The successful act of bypassing the security mechanisms; the unauthorized access to an automated system." (AFCERT Computer Glossary)

Penetration signature: "The description of a situation or set of conditions in which a penetration could occur or of system events which in conjunction can indicate the occurrence of a penetration in progress." (AFCERT Computer Glossary)

Probe: "Any effort to gather information about a machine or its users on-line for the apparent purpose of gaining unauthorized access to the system at a later date." (AFCERT Computer Glossary)

Proxy: "A firewall mechanism that replaces the IP address of a host on the internal (protected) network with its own IP address for all traffic passing through it. A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination." (AFCERT Computer Glossary)

Pseudo-flaw: "An apparent loophole deliberately implanted in an operating system program as a trap for intruders." (AFCERT Computer Glossary)

Retro-virus: "A retro-virus is a virus that waits until all possible backup media are infected too, so that it is not possible to restore the system to an uninfected state." (AFCERT Computer Glossary)

Session hijacking: "Taking over an authorized user's terminal session, either physically when the user leaves his terminal unattended or electronically when the

intruder carefully connects to a just-disconnected communications line.” (AFCERT Computer Glossary)

Sniffer: “A tool used to intercept potentially exploitable data from the traffic on a network. A program to capture data across a computer network. Used by hackers to capture user id names and passwords. Software tool that audits and identifies network traffic packets.” (AFCERT Computer Glossary)

Social engineering: “An attack based on deceiving users or administrators at the target site. Social engineering attacks are typically carried out by telephoning users or operators and pretending to be an authorized user, to attempt to gain illicit access to the systems.” (AFCERT Computer Glossary)

Spoofing: “Pretending to be someone else. The deliberate inducement of a user or a resource to take an incorrect action. Attempt to gain access to an AIS by pretending to be an authorized user. Impersonating, masquerading, and mimicking are forms of spoofing.” (AFCERT Computer Glossary)

Technical attack: “An attack that can be perpetrated by circumventing or nullifying hardware and software protection mechanisms, rather than by subverting system personnel or other users.” (AFCERT Computer Glossary)

Technical Vulnerability: “A hardware, firmware, communication, or software flaw that leaves a computer processing system open for potential exploitation, either externally or internally, thereby resulting in risk for the owner, user, or manager of the system.” (AFCERT Computer Glossary)

Trap door: "A hidden software or hardware mechanism used to circumvent security control." (AFCERT Computer Glossary)

Trojan horse: "An apparently useful and innocent program containing additional hidden code which allows the unauthorized collection, exploitation, falsification, or destruction of data." (AFCERT Computer Glossary)

van Eck monitoring: Monitoring the activity of a computer or other electronic equipment by detecting low levels of electromagnetic emissions from the device. Named after Dr. Wim van Eck who published on the topic in 1985.⁷ See emanations.

Virus: "A variation of Trojan Horse. It is propagating with a triggering mechanism (event time) with a mission (delete files, corrupt data, send data). Often self replicating, malicious program segment that attaches itself to an application program or other executable system component and leaves no obvious signs of its presence." (AFCERT Computer Glossary)

Vulnerability: "Hardware, firmware, or software [flaw] that leaves a computer processing system open for potential exploitation. A weakness in automated system security procedures, administrative controls, physical layout, internal controls, and so forth, that could be exploited by a threat to gain unauthorized access to information or disrupt critical processing." (AFCERT Computer Glossary)

War dialer: "A cracking tool, a program that calls a given list or range of numbers and records those which answer with handshake tones (and so might be entry points to computer or telecommunications systems)." (AFCERT Computer Glossary)

Worm: "A program or executable code module which resides in distributed systems or networks. It will replicate itself, if necessary, in order to exercise as much of the system's resources as possible for its own processing. Such resources may take the form of CPU time, I/O channels, or system memory. It will replicate itself from machine to machine across network connections, often clogging networks and computer systems as it spreads."(AFCERT Computer Glossary)

⁷ Russell and Gangemi 254.

APPENDIX C. SOF MISSIONS AND COLLATERAL ACTIVITIES

Joint Pub 3-05, *Doctrine for Joint Special Operations*, defines special operations (SO) as "Operations conducted by specially organized, trained, and equipped military and paramilitary forces to achieve military, political, economic, or psychological objectives by unconventional military means in hostile, denied, or politically sensitive areas. These operations are conducted...[across the range of military operations], independently or in coordination with operations of conventional, non-special operations forces (SOF). Political-military considerations frequently shape SO, requiring clandestine, covert, or low visibility techniques, and oversight at the national level. SO differ from conventional operations in degree of physical and political risk, operational techniques, mode of employment, independence from friendly support, and dependence on detailed operational intelligence and indigenous assets." This appendix provides definitions of the SOF Principal Missions and Collateral Activities as they appear in the 1998 USSOCOM Posture Statement. Section 167 of title 10, of the US Code defines 10 special operation activities.

A. PRINCIPAL MISSIONS

Counterproliferation (CP) — The activities of the Department of Defense across the full range of U.S. government efforts to combat proliferation of nuclear, biological, and chemical weapons, including the application of military power to protect U.S. forces and interests; intelligence collection and analysis; and support of diplomacy, arms

control, and export controls. Accomplishment of these activities may require coordination with other U.S. government agencies.

Combating terrorism (CBT) — Preclude, preempt, and resolve terrorist actions throughout the entire threat spectrum, including antiterrorism (defensive measures taken to reduce vulnerability to terrorist acts) and counter-terrorism (offensive measures taken to prevent, deter, and respond to terrorism), and resolve terrorist incidents when directed by the National Command Authorities or the appropriate unified commander or requested by the Services or other government agencies.

Foreign internal defense (FID) — Organize, train, advise, and assist host nation military and para-military forces to enable these forces to free and protect their society from subversion, lawlessness, and insurgency.

Special reconnaissance (SR) — Conduct reconnaissance and surveillance actions to obtain or verify information concerning the capabilities, intentions, and activities of an actual or potential enemy or to secure data concerning characteristics of a particular area.

Direct action (DA) — Conduct short-duration strikes and other small-scale offensive actions to seize, destroy, capture, recover, or inflict damage on designated personnel or materiel.

Psychological operations (PSYOP) — Induce or reinforce foreign attitudes and behaviors favorable to the originator's objectives by conducting planned operations to convey selected information to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

Civil affairs (CA) — Facilitate military operations and consolidate operational activities by assisting commanders in establishing, maintaining, influencing, or exploiting relations between military forces and civil authorities, both governmental and non-governmental, and the civilian population in a friendly, neutral, or hostile area of operation.

Unconventional warfare (UW) — Organize, train, equip, advise, and assist indigenous and surrogate forces in military and paramilitary operations normally of long duration.

Information operations (IO) — Actions taken to achieve information superiority by affecting adversary information and information systems while defending one's own information and information systems.

B. COLLATERAL ACTIVITIES

Coalition support — Integrate coalition units into multinational military operations by training coalition partners on tactics and techniques and providing communications.

Combat search and rescue (CSAR) — Penetrate air defense systems and conduct joint air, ground, or sea operations deep within hostile or denied territory at night or in adverse weather to recover distressed personnel during wartime or contingency operations. SOF are equipped and manned to perform CSAR in support of SOF missions only. SOF perform CSAR in support of conventional forces on a case-by-case basis not to interfere with the readiness or operations of core SOF missions.

Counterdrug (CD) activities — Train host nation CD forces and domestic law enforcement agencies on critical skills required to conduct individual and small unit operations in order to detect, monitor, and interdict the cultivation, production, and trafficking of illicit drugs targeted for use in the United States.

Humanitarian demining (HD) activities — Reduce or eliminate the threat to noncombatants and friendly military forces posed by mines and other explosive devices by training host nation personnel in their recognition, identification, marking, and safe destruction. Provide instruction in program management, medical, and mine awareness activities.

Humanitarian assistance (HA) — Provide assistance of limited scope and duration to supplement or complement the efforts of host nation civil authorities or agencies to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to, or loss of, property.

Peace operations — Assist in peacekeeping operations, peace enforcement operations, and other military operations in support of diplomatic efforts to establish and maintain peace.

Security assistance (SA) — Provide training assistance in support of legislated programs which provide U.S. defense articles, military training, and other defense-related services by grant, loan, credit, or cash sales in furtherance of national policies or objectives.

Special activities — Subject to limitations imposed by Executive Order and in conjunction with a Presidential finding and congressional oversight, plan and conduct actions abroad in support of national foreign policy objectives so that the role of the U.S. government is not apparent or acknowledged publicly.

APPENDIX D. IW/IO DEFINITIONS

This appendix provides a list of various definitions of IO, IW, and related concepts.

A. INFORMATION WARFARE:

1. "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks." (*Joint Publication 1-02, DOD Dictionary of Military and Associated Terms.*)

2. "Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries." (*DoD Instruction 3600.1*)

3. "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks." (Dept. of the Army, *FM 100-6 Information Operations*).

4. "Information operations conducted to defend one's own information and information systems or attacking and affecting an adversary's information and information systems. The defensive aspect, *defensive counterinformation, much like strategic air defense*, is always operative. *Conversely*, the offensive aspect, *offensive*

counterinformation, is primarily conducted during times of crisis or conflict.” (Italics original) (Dept. of the Air Force, *AFDD 25 Information Operations*)

5. “Hostile activity directed against any part of the knowledge and belief systems of an adversary.” (Szafranski, *A Theory of Information Warfare*)

6. “Type I Information Warfare involves managing the enemy’s perceptions. Type II Information Warfare involves denying, destroying, degrading, or distorting the enemy’s information flows in order to break down his organizations and his ability to coordinate operations. Type III Information Warfare gathers intelligence by exploiting the enemy’s use of information systems.” (Michael L. Brown, “The Revolution in Military Affairs: the Information Dimension,” *Cyberwar: security, Strategy and Conflict in the Information Age*, Alan D Campen, Douglas H. Dearth, R. Thomas Gooden, eds. (Fairfax: AFCEA International Press, 1996).

7. “The preparation for and use of physical and logic-based weapons that disrupt or destroy information or information systems in order to degrade or disrupt information function(s) that depend on the information and information systems.” (Thomas Knecht, “Thoughts on Information Warfare” in *Cyberwar: Security, Strategy, and Conflict in the Information Age*).

8. “The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives.” (Thomas Rona, quoted in Martin Libicki, *What is Information Warfare*).

9. "Information warfare is a conflict in which a combat-ready military (as well as political, economic, cultural and technological) units employ force to occupy the infosphere and dispute each other's access to information resources. This refers chiefly to activities whereby a state employs information for the purpose of attaining strategic objectives." (Shen Weiguang, "Information Warfare – A New Challenge")

10. "Information warfare, in its essence, is about *ideas and epistemology*- big words meaning that information warfare is about the way humans think and, more important, the way humans make decisions. And although information warfare would be waged largely, but not entirely, through the communication nets of a society or its military, it is fundamentally not about satellites, wires, and computers. It is about influencing human beings and the decisions they make." (George Stein, "Information Warfare")

11. "An electronic conflict in which information is a strategic asset worthy of conquest or destruction." (Schwartau, *Chaos on the Information Superhighway* 1994)

B. INFORMATION OPERATIONS

1. "Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW"(Dept. of Defense, *Joint Pub 3-13 Joint Doctrine for Information Operations*, 1998)

2. "Actions taken to deny, exploit, corrupt, or destroy the enemy's information and its functions, protecting ourselves against those actions, and exploiting our own information operations." (Dept. of the Air Force, *Cornerstones of Information Warfare*)

3. "Actions taken to gain, exploit, defend, or attack information and information systems. In-formation operations apply across the range of military operations, from peace to all-out conflict." (Dept. of the Air Force, *AFDD 25 Information Operations*)

4. "Those actions taken to gain, exploit, defend or attack information and information systems and include both information-in-warfare and information warfare." (This is a "working definition" that applies only to the Air Force.) (Dept. of the Air Force, *AFDD 25 Information Operations*).

5. "Continuous military operations within the military information environment that enable, enhance, and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the global information environment and exploiting or denying an adversary's information and decision capabilities" (Dept. of the Army, *FM 100-6 Information Operations*).

6. "Offensive and defensive warfighting actions in or via the information environment to control and exploit that realm." (Dan Kuehl, "Defining Information Power" *INSS Strategic Forum*, Number 115, June 1997)

C. OTHER DEFINITIONS

1. Cyberwar: "Conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting, if not destroying,

information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, and so forth. It means trying to know everything about an adversary while keeping the adversary from knowing much about oneself. It means turning the "balance of information and knowledge" in one's favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended." (Arquilla and Ronfeldt, *Cyberwar is Coming!*)

2. Netwar: "Netwar refers to an information-related conflict at a grand level between nations or societies. It means trying to disrupt, damage, or modify what a target population "knows" or thinks it knows about itself and the world around it. A netwar may focus on public or elite opinion, or both. It may involve public diplomacy measures, propaganda and psychological campaigns, political and cultural subversion, deception or interference with local media, infiltration of computer networks and databases, and efforts to promote dissident or opposition movement across computer networks." (Arquilla and Ronfeldt, *Cyberwar is Coming!*)

3. C2W: "The military strategy that implements Information Warfare on the battlefield and integrates physical destruction. Its objective is to decapitate the enemy's command structure from its body of troops." (Dept. of Defense, CJCS MOP-30, 1993)

4. C2W: "The integrated use of physical psychological operations, military deception, operations security, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary

C2 capabilities while protecting friendly C2 capabilities against such actions.” (Dept. of Defense, *Joint Pub 3-13.1 Joint Doctrine for Command and Control Warfare*, 1995)

BIBLIOGRAPHY

- Allard, C. Kenneth. "The Future of Command and Control: Toward a Paradigm of Information Warfare" in *Turning Point: The Gulf War and U.S. Military Strategy*. L. Benjamin Ederington and Michael J. Mazarr, eds. (San Francisco: Westview Press, 1995).
- . "Information Operations in Bosnia: A Preliminary Assessment." *INSS Strategic Forum* Number 91, November 1996. Online. Internet. Available: www.ndu.edu/inss/strforum/h6.html
- Arquilla, John and David Ronfeldt. *Cyberwar is Coming! Comparative Strategy*, Vol. 12, pp. 141-165, 1993. Reprinted in *In Athena's Camp: Preparing for Conflict in the Information Age* (Santa Monica: Rand, 1997).
- . "Preparing for Information-Age Conflict." *Information, Communication & Society* 1:1 Spring 1998: 1-22 and 1:2 Summer 1998: 121-143.
- . *The Advent of Netwar* (Santa Monica: Rand, 1996).
- Arquilla, John and Solomon M. Kamel. "Welcome to the Revolution...in Chinese Military Affairs" *Defense Analysis* 1997 Vol. 13, No. 3: pp.257-270.
- Arquilla, John. "Bound to Fail." *Comparative Strategy*. 1995, v.14 n.12: 123-135.
- . "The Great Cyberwar of 2002." *Wired* Issue 6.02, February 1998, n.pag. Online. Internet. Available: www.wired.com/wired/6.02/cyberwar.htm
- . "The Strategic Implications of Information Dominance." *Strategic Review* Summer 1994: 24-30.
- . "The "Velvet" Revolution in Military Affairs." *World Policy Journal*. Winter 1997/98, Vol. XIV, No. 4, pp.32-43.
- Atkeson, Edward B. "Shudder of Nukes on the Subcontinent." *Army* August 1998:18-24.
- Barnett, Roger W. "Information Operations, Deterrence, and the Use of Force." *Naval War College Review*. Spring 1998: 7-19.
- Berardinelli, Thomas F. et. al. "Surfing the First and Second Waves in 2025: A SOF Strategy for Regional Engagement." *Air Force 2025* Vol. 3, Book 10. Air University, August 1996. Online. Internet. Available: tuvok.au.af.mil/au/2025/
- Beres, Louis Rene. "Preventing Nuclear Terrorism Against the United States: 10 Vital Questions" *Special Warfare* August 1996: 22-29.
- Berkowitz, Bruce. "Warfare in the Information Age," *Issues in Science and Technology*, Fall 1995: 59-66. Copyright 1995 by the University of Texas at Dallas, Richardson, TX.

- Blackburn, Dale A., et. al. *A National Policy For Deterring The Use Of Weapons Of Mass Destruction*. Research Paper, Air Command and Staff College, April 1996. Online. Internet. Available: www.au.af.mil/au/database/research/ay1996/acsc/96-102.htm
- Bond, Brian. *Liddell Hart: A Study of His Military Thought*. (New Brunswick: Rutgers University Press, 1976).
- Brennan, Rick and R. Evan Ellis. *Information Warfare in Multilateral Peace Operations - A Case Study of Somalia*. 18 April 1996. Prepared for the Office of the Secretary of Defense, Net Assessment by Science Applications International Corporation (SAIC). Online. Internet. Available: sac.saic.com/industrial_base_assessments/information_warfare/somalia.htm
- Buchan, Glenn. *Information War and the Air Force: Wave of the Future? Current Fad?* Rand Issue Paper: Project Air Force. March 1996. n.pag. Online. Internet. Available: www.rand.org
- Campen, Alan D., Douglas H. Dearth, R. Thomas Gooden, eds. *Cyberwar: security, Strategy and Conflict in the Information Age* (Fairfax: AFCEA International Press, 1996).
- Centner, Christopher M. "Precision-Guided Propaganda: Exploiting the U.S. Information Advantage in Peacetime." *Strategic Review* Spring 1997: 35-41.
- Cerniglia, James A. et. al. "The Dim Mak Response of Special Operations Forces to the World of 2025: 'Zero Tolerance/Zero Error.'" *Air Force 2025* Vol. 3, Book 11. Air University. August 1996. Online. Internet. Available: tuvok.au.af.mil/au/2025/
- Clinton, William J. "Remarks At The United States Naval Academy Commencement" United States Naval Academy. Annapolis, Maryland May 22, 1998. Online. Internet. Available www.pub.whitehouse.gov
- Cohen, Eliot. "A Revolution in Warfare." *Foreign Affairs*. March/April 1996, p37-54.
- Collins, John M. *Special Operations Forces: An Assessment*. (Washington D.C.: NDU Press, 1994).
- Czerwinski, Thomas J. "The Third Wave: What the Toffler's Never Told You." *INSS Strategic Forum* Number. 72, April 1996. Online. Internet. Available: www.ndu.edu/inss/strforum/h6.html
- Department of the Air Force. *Cornerstones of Information Warfare*. Washington, D.C.: Department of the Air Force, 1996. Online. Internet. Available: www.af.mil/lib/corner.html
- . *AFDD 1: Air Force Basic Doctrine* (Washington, D.C.: Department of the Air Force, 1997).

- . *AFDD 2-5: Information Operations* (Washington, D.C.: Department of the Air Force, 1998).
- . *AFDD 35: Special Operations*. (Washington, D.C.: Department of the Air Force) 16 January 1995.
- Department of the Army, *Field Manual 100-5-1, Operational Terms and Graphics*. (Washington D.C.: Department of the Army, 1997).
- . *Field Manual 100-6, Information Operations* (Washington, D.C.: Department of the Army, 1996).
- *Army Special Operations: Vision 2010* (Washington, D.C.: U.S. Army Special Operations Command, 1997). Reprinted in *Special Warfare* Fall 1997: 34-41.
- . *Army Vision 2010*. (Washington, D.C.: Department of the Army, 1996).
- Department of Defense, *Annual Report to the President and the Congress* (Washington D.C.: Dept. of Defense, 1998). Online. Internet. Available: www.dtic.mil/execsec/ad98
- . *Concept for Future Joint Operations: Expanding Joint Vision 2020* (Washington D.C.: Dept. of Defense (JCS), May 1997).
- . *Joint Publication 1-02, DoD Dictionary Military and Associated Terms* (Washington, D. C.: Dept. of Defense, 1998). Online. Internet. Available: www.dtic.mil/doctrine/jel/doddict/
- . *Joint Publication 3-05, Doctrine for Joint Special Operations* (Washington, D.C.: Dept. of Defense, April 1998). Online. Internet. Available: www.dtic.mil/doctrine/jel/
- . *Joint Pub 3-53, Doctrine for Joint Psychological Operations* (Washington, D.C.: GPO, 1996).
- . *Joint Vision 2010* (Washington, D.C.: Dept. of Defense, 1995). Online. Internet. Available: www.army.mil/2010
- . *Quadrennial Defense Review* (Washington D.C.: Dept. of Defense, May 1997). Online. Internet. Available: www.defenselink.mil/pubs/qdr/.
- . *SOF Vision 2020* (Washington, D.C.: Dept. of Defense (USSOCOM), 1996).
- . *United States Special Operations Forces: Posture Statement 1998*. (Washington, D.C.: Dept. of Defense (OSD-SO/LIC), 1998).
- . *USSOCOM Pub 1: Special Operations in Peace and War* (Washington, D.C.: Dept. of Defense (USSOCOM), 1996).
- DiNardo R. L. and Daniel J. Hughes. "Some Cautionary Thoughts on Information Warfare." *Air Power Journal* No. 4 Winter 1995: 69-79. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/apj/wint95.html

- Doherty, Terry. "SOF Roles and Missions: Re-examining the Environment" *Special Warfare* May 1993: 21-23.
- Dunlap, Charles J. Jr. "21st Century Land Warfare: Four Dangerous Myths" *Parameters*, Autumn 1997: 27-37.
- . "Organizational Change and The New Technologies of War." Jan 30, 1998. Paper presented to the Joint Services Conference on Professional Ethics (JSCOPE) Washington, D.C. Online. Internet. Available: www.usafa.af.mil/jscope/Dunlap98.htm
- Dredla, Michael J. *Commando Vision: A Strategic Vision for Air Force Special Operations Command*. Air War College, April 1997. Online. Internet. Available: www.au.af.mil/au/database/research/ay1997/awc/97-054.htm
- Edwards, Sean J. A. "The Threat of High Altitude Electromagnetic Pulse to Force XXI." *National Security Studies Quarterly*. Autumn 1997, Vol. III, Issue 4. p. 61-79.
- Ellul, Jacques. *Propaganda: The Formation of Men's Attitudes*. (New York: Knopf, 1965).
- Freedman, Lawrence - *Information Warfare: Will Battle Ever Be Joined?*. Lecture given at the Launch of International Centre for Security Analysis (ICSA), 14 October, 1996. n.pag. London. Online. Internet. Available: www.Infowar.Com/mil_c4i/icsa/icsa1.html-ssi
- Garrison, William F. and Hayward S. Florer, Jr. "A View from the Field: Army Special Operations Forces in the Current and Future Security Environments" *Special Warfare* May 1996: 8-15.
- Given, Kevin. "Luddites, the RMA, and Doctrine." *Research and Analysis* July 1996: n.pag. Online. Internet. Available: www.adfa.oz.au/dod/dara/issue08.htm
- Goldstein, Frank L. ed. *Psychological Operations: Principals and Case Studies*. (Maxwell AFB: Air University Press, 1996).
- Gottlieb, Aryea. "The Role of SOF Across the Range of Military Operations." Online. Internet. Available: www.cadre.maxwell.af.mil/airchronicles/cc/sofpaper.html
- Gourley, Robert D. "The Devil is in the Details." *United States Naval Institute Proceedings* Sep 1997: 86-88. Online. Proquest.
- Gray, Colin S. *Explorations in Strategy* (Westport: Greenwood Press, 1996).
- . "RMAs and the Dimensions of Strategy." *Joint Forces Quarterly*. Autumn/Winter 1997-98: 50-54.
- Greenberg, Lawrence T., Seymour E. Goodman and Kevin J. Soo Hoo. *Information Warfare and International Law*. Washington, D.C.: National Defense University Press, 1998. n.pag. Online. Internet. Available: www.dodccrp.org/iwilindex.htm

- Hamseman, Robert G. "The Realities and Legalities of Information Warfare." *The Air Force Law Review* 1997 42: 173-200. Online. Proquest.
- Hayes, Richard E. and Gary Wheatley "Information Warfare and Deterrence" *INSS Strategic Forum* Number 87, October 1996. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum
- Holmes, H. Allen, "Military Operations in the Post Cold War Era" Speech. Intelligence in Partnership Conference, Joint Military Intelligence Conference, Andrews AFB Maryland, June 26, 1997. Reprinted in *Defense Issues* Vol. 12, No. 34. Available: www.defenselink.mil/speeches/1997/di1234.html
- Howard Stephen P. *Special Operations Forces And Unmanned Aerial Vehicles: Sooner Or Later?* School Of Advanced Airpower Studies Air University Maxwell Air Force Base, Alabama June 1995.
- Howle, Timothy E. "Information Operations: The Role of Civil Military Operations and Civil Affairs" *Special Warfare* Spring 1997: 16-17.
- Johnsen, William T., et. al. *The Principles of War in the 21st Century: Strategic Considerations*. US Army Strategic Studies Institute, 1995. n.pag. Online. Internet. Available: carlisle-www.army.mil/usassi/ssipubs/pubs95/pow21/pow21tc.htm
- Knecht, Ronald J. "Thoughts on Information Warfare" in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds. (Fairfax: AFCEA International Press, 1996).
- Kuehl, Dan. "Defining Information Power." *INSS Strategic Forum* Number 115, June 1997. n.pag. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum
- "Information and Nuclear RMAs Compared" *INSS Strategic Forum* Number 82, July 1996. Online. Internet. Available www.ndu.edu/inss/strforum
- . "Information Dominance" *INSS Strategic Forum* Number 132, November 1997. Online. Internet. Available www.ndu.edu/inss/strforum.
- . "Defining Information Warfare." *The Officer* November 1997: 31-33.
- . "Joint Information Warfare" *INSS Strategic Forum* Number 105, March 1997. n.pag. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum
- Krepinevich, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions," *The National Interest* Fall 1994: 30 - 41.
- Larson, Eric V. *Casualties and Consensus: The Historical Role of Casualties in Domestic Support for U.S. Military Operations* (Santa Monica: Rand, 1996).
- Leonard-Barxton, D. "Core Capabilities and Core Rigidities: A Paradox in Managing New Product Development." *Strategic Management Journal* 1992, v13: 111-125.

- Libicki, Martin. *What is Information Warfare?* (Washington, D.C.: National Defense University Press, 1995). Online. Internet. Available: www.ndu.edu/inss/actpubs/act003/a003cont.html
- "Information Dominance" *INSS Strategic Forum* Number 132, November 1997. n.pag. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum
- Libicki, Martin and Stuart Johnson, eds. *Dominant Battlespace Knowledge* (Washington D.C.: NDU Press, October 1995). Online. Internet. Available: www.ndu.edu/ndu/inss/books/dbk/dbk1.html
- Mann, Edward. "Desert Storm: The First Information War?" *Air Power Journal* Vol. VIII, No. 4 (Winter 1994): 4-14. Online. Internet. Available: www.cadre.maxwell.af.mil/airchronicles/apj/apj94/win94.html
- Mason, R. A. "Innovation and the Military Mind." *Air University Review* January-February 1986. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/aureview/1986/jan-feb
- Miller, John H. *Information Warfare: Issues and Perspectives*. (Carlisle: NDU Press (INSS)). Online. Internet. Available: www.ndu.edu/inss/siws/ch7.html
- McKittrick, Jeffery, et. al. *The Revolution in Military Affairs*. SAIC Strategic Assessment Center, 1994. Online. Internet. Available: sac.saic.com/rma/rmapaper.htm
- McLendon, James W. "Information Warfare: Impacts and Concerns." *Battlefield of the Future: 21st Century Warfare Issues*. Air War College. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/battle/chp7.html
- McRaven, William H. *Spec Ops - Case studies in Special Operations Warfare: Theory and Practice* (Novato: Presidio Press, 1995).
- Metz, Steven. "A Wake for Clausewitz: Toward a Philosophy of 21st-Century Warfare" *Special Warfare* October 1995: 22-28.
- Molander, Roger, Andrew S. Riddile, and Peter A. Wilson. *Strategic Information Warfare: A New Face of War* (Santa Monica: Rand, 1996). Also available online at www.rand.org/publications/mr/mr661/mr661.html
- Morris, Chris, Janet Morris and Thomas Baines, "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos." *Air Power Journal* Spring 1995: 15-29. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/apj/spr95.html
- Murphy, Edward F. et. al. "Information Operations: Wisdom Warfare for 2025." *Air Force 2025*. Vol. 3, Book 3. Air University. August 1996. Online. Internet. Available: tuvok.au.af.mil/au/2025
- National Defense Panel. *Transforming Defense: National Security in the 21st Century*. (Washington D.C.: National Defense Panel, 1997). Online. Internet. Available: www.dtic.mil/ndp

- Nye, Joseph S. Jr. and William A. Owens. "America's Information Edge" *Foreign Affairs* March April 1996: 20-36.
- Osborne, William B. et. al. "Information Operations: A New War Fighting Capability" *Air Force 2025* Vol. 3 Book 2. Air University, August 1996. Online. Internet. Available: tuvok.au.af.mil/au/2025
- Pfaltzgraff, Robert L. "Sources of Instability: Implications for Special operations Forces" *Special Warfare* October 1995: 2-9.
- Pfaltzgraff, Robert L. and Richard H. Schultz, eds., *War in the Information Age* (Washington D. C.: Brassey's, 1996).
- Pillsbury, Michael, ed. *Chinese Views of Future Warfare* (Washington D.C.: NDU Press, 1997). Online. Internet. Available: www.ndu.edu/ndu/inss/books/books.html
- Prahalad, C.K. and Gary Hamel. "The Core Competence in the Corporation" *Harvard Business Review* May-June 1990: 79-91.
- Research Planning, Inc. "Regional Engagement: A Concept Paper." Unpublished paper prepared for the U.S. Army John F. Kennedy Special Warfare Center. 1996.
- Rodgers, James L. "Information Warfare: Nothing New under the Sun." *Marine Corps Gazette* Apr 1997: 23-29.
- Rothrock, John. "Information Warfare: Time for Some Constructive Skepticism?" in *Athena's Camp: Preparing for Conflict in the Information Age*. John Arquilla and David Ronfeldt, eds. Santa Monica: Rand, 1997. Prepared for the Office of the Secretary of Defense by RAND's National Defense Research Institute.
- Salisbury Harrison Evans, *The 900 Days: The Siege of Leningrad* (Da Capo Press: New York, 1985).
- Schoomaker, Peter J. "U.S. Special Operations Forces: The Way Ahead." *Special Warfare* Winter 1998: 2-9.
- Schwartz, Winn. *Information Warfare: Chaos on the Electronic Superhighway*, 2nd ed. (New York: Thunder's Mouth Press, 1995).
- Sepp, Kalev I. "Preparing for 2010: Thinking Outside the 'War Box'" *Special Warfare* Winter 1997: 2-6.
- Shafritz, Jay M. ed. *Words on War* (New York: Prentice Hall, 1990).
- Shelton, Henry H. "Special Operations Forces: Key Role in Preventive Defense" *Defense Issues*, 1997 Vol. 12, No. 12, Washington D.C.: Armed Forces Information Service, Washington, D. C.
- "Special Operations Forces: Looking Ahead" *Special Warfare* Spring 1997: 2-11.
- Singer, Abe and Scott Rowell. "Information Warfare: An Old Operational Concept with New Implications." *INSS Strategic Forum* Number 99, December 1996. Online. Internet. Available: www.ndu.edu/ndu/inss/strforum

- Smith, George. "Truth is the First Casualty of Cyberwar." *Wall Street Journal*. September 8, 1998. p A28.
- Stein, George J. "Information Attack: Information Warfare in 2025." *Air Force 2025* Vol.3, Book 1. Air University. August 1996. Online. Internet. Available: tuvok.au.af.mil/au/2025
- "Information Warfare" in *Cyberwar: Security, Strategy, and Conflict in the Information Age*. Alan D. Campen, Douglas H. Dearth, and R. Thomas Gooden, eds. (Fairfax: AFCEA International Press, 1996).
- "Information War-Cyberwar-Netwar." *Battlefield of the Future: 21st Century Warfare Issues*. Barry R. Schneider and Lawrence E. Grinter Eds. Maxwell AFB: Air War College, September 1995. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/battle/front.html
- Stocker, Gerfried and Christine Schopf, eds., *Infowar*, (New York: Springer Wein/ ARS Electronica, 1998).
- Sullivan, Brian. "Special Operations and LIC in the 21st Century: The Joint Strategic Perspective" *Special Warfare* May 1996: 1-7.
- "The Future National Security Environment: Possible Consequences for Army SOF" *Special Warfare* August 1996: 2-12.
- Sun Tzu. *The Art of War*, Trans. Samuel Griffith, (New York: Oxford, 1963).
- Szafranski, Richard. "An Information Warfare SIIOP" (n.pub) Online. Internet. Available: www.infowar.com/mil_c4i/szafran.html-ssi
- "A Theory of Information Warfare: Preparing for 2020." *Air Power Journal* Vol. 9. No. 1 Spring 1995: 56-65. Online Internet. Available: www.cadre.maxwell.af.mil/airchronicles/apj/spr95.html
- "Neocortical Warfare? The Acme of Skill." *Military Review* Vol. 74, no. 11 November 1994: 41-55. Also available in *In Athena's Camp: Preparing for Conflict in the Information Age*. John Arquilla and David Ronfeldt, eds. (Santa Monica: Rand, 1997).
- "Parallel War and Hyperwar: Is Every Want a Weakness?" *Battlefield of the Future: 21st Century Warfare Issues*. Barry R. Schneider and Lawrence E. Grinter Eds. (Maxwell AFB: Air War College, September 1995).n.pag. Online. Internet. Available: www.airpower.maxwell.af.mil/airchronicles/battle/front.html
- "Twelve Principles Emerging From Ten Propositions." *Airpower Journal* Spring 1996: 72-80.
- Thomas, Timothy L. "Deterring Information Warfare: A New Strategic Challenge." *Parameters* Winter 1996-97: 81-91. Also available online: carlisle-www.army.mil/usawc/Parameters/96winter/thomas.htm

- .“Russian Views On Information-Based Warfare.” *Air Power Journal* July 1996
Special Edition: pp.25-34. Online. Internet Available:
www.airpower.maxwell.af.mil/airchronicles/apj/thomas.html
- .“The Mind Has No Firewall.” *Parameters* Spring 1998: 84-92. Also available online:
carlisle-www.army.mil/usawc/Parameters/98spring/thomas.htm
- . “The Age of the New Persuaders.” *Military Review*. May-June 1997: pp72-80. .
Also available online: www-cgsc.army.mil/milrev/english/novdec97/index97.htm
- .“A Threat of Information Operations: A Russian Perspective.” *War in the Information Age*. Pfaltzgraff, et. al. eds. (Washington, D. C.: Brassey’s, 1996). 61-79.
- Thrasher, Robert D. *Information Warfare: Implications for Forging the Tools*. Thesis Naval Postgraduate School. Monterey. June 1996.
- Tilford, Earl H. Jr. ed. *World View: The 1998 Strategic Assessment from the Strategic Studies Institute* (Carlisle Barracks: US Army War College, 1998).
- Toffler, Alvin and Heidi Toffler. *War and Anti-War: Making Sense of Today’s Global Chaos* (New York: Warner, 1995).
- United States. *A National Security Strategy for A New Century May 1997*. Washington, D. C.: United States, 1997. Online. Internet. Available:
www.whitehouse.gov/wh/eop/nsc/strategy/
- .*Critical Foundations: Protecting America’s Infrastructure* (Washington, D.C.: President’s Commission on Critical infrastructure Protection, 1997). Online. Internet. Available: www.pcip.org
- .*Special Operations Forces: Opportunities to Preclude Overuse and Misuse*. Report to the Chairman, Subcommittee on Military Readiness, Committee on National Security, House of Representatives. (Washington, D.C.: General Accounting Office, 1997).
- van Creveld, Martin. *Command in War* (Cambridge: Harvard University Press, 1985).
- Waltz, Edward. *Information Warfare: Principles and Operations* (Boston: Artech House, 1998).
- Wilson, Michael. “Battle for the Soul of Information Warfare: Pearl Harbor vs. The Hashishim.” 1996. Online. Internet. Available: www.7pillars.com/papers
- Zhenxing, Liang. “China: New Military Revolution, Information Warfare” Text from address translated by the Foreign Broadcast Information Service (FBIS). 12 Jan 1998.
- Zimm, Alan D. “Deterrence: Basic Theory, Principles, and Implications.” *Strategic Review* Spring 1997: 42-50.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
8725 John J. Kingman Rd., Ste 0944
Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
Naval Postgraduate School
411 Dyer Rd
Monterey, CA 93943-5101

3. Professor Gordon H. McCormick 1
Code CC/Mc
Naval Postgraduate School
Monterey, CA 93943-5000

4. Professor John Arquilla 1
Code CC
Naval Postgraduate School
Monterey, CA 93943

5. The Honorable H. Allen Holmes 1
Assistant Secretary of Defense for SO/LIC
The Pentagon, RM 2E258
Washington, DC 20301-2500

6. GEN Peter J. Schoomaker 1
Commander in Chief
US Special Operations Command
MacDill AFB, FL 33608-6001

7. LTG William Tangney 1
Commander
US Army Special Operations Command
Ft. Bragg, NC 28307-5000

8. RADM Thomas R. Richards 1
Commander
Naval Special Warfare Command
NAB Coronado
San Diego, CA 92155

9. MG Charles R. Holland 1
Commander
Air Force Special Operations Command
Hurlburt Field, FL 32544

10. MG Bryan Brown.....	1
Commander	
Joint Special Operations Command	
Ft. Bragg, NC 29307	
11. Jennifer Duncan.....	5
Center for Special Operations	
Code (CC/Jd)	
Naval Postgraduate School	
Monterey, CA 93943-5000	
12. Library.....	1
Army War College	
Carlisle Barracks, PA.17013	
13. Library.....	1
Naval War College	
Newport, RI 02840	
14. Strategic Studies Group (SSG)	1
Naval War College	
Newport, RI 02840	
15. Department of Military Strategy.....	1
National War College (NWMS)	
Ft. Leslie J. McNair	
Washington, DC 20319-6111	
16. US Army Command and General Staff College	1
ATTN: Library	
Ft. Leavenworth, KS 66027-6900	
17. Library.....	1
Air War College	
Maxwell AFB, AL 36112-6428	
18. US Military Academy	1
ATTN: Library	
West Point, NY 10996	
19. US Naval Academy.....	1
ATTN: Library	
Annapolis, MD 21412	
20. Maraquat Memorial Library	1
US Army John F. Kennedy Special Warfare Center	
Rm. C287, Bldg. 3915	
Ft. Bragg, NC 28307-5000	

21. Commander 1
Naval Special Warfare Group One
NAB Coronado
San Diego, CA 92155
22. Commander 1
Naval Special Warfare Group Two
NAB Little Creek, VA 23521
23. Commander 1
Naval Special Warfare Center
NAB Coronado
San Diego, CA 92155
24. US Special Operations Command 1
ATTN: Command Historian
MacDill AFB, FL 33608-6001
25. Commander 1
USJFKSWCS
Ft. Bragg, NC 28307-5000
26. COL J. Lawton.....1
USSOCOM/SOIO
7701 Tampa Point Blvd
MacDill AFB, FL 33621-5353
27. MAJ Scott Moore.....1
Future Concepts Working Group
USSOCOM/SOOP-SF
7701 Tampa Point Blvd
MacDill AFB, FL 33621-5353

DTIC QUALITY INSPECTED 4