Calhoun
Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

1996-06

Attacking the infrastructure: exploring potential uses of offensive information warfare

Elam, Donald Emmett.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/32073

DUDLEY KNOX LIBRARY

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA

THESIS

ATTACKING THE INFRASTRUCTURE: EXPLORING POTENTIAL USES OF OFFENSIVE INFORMATION WARFARE

by

Donald Emmett Elam

June, 1996

Thesis Co-Advisors: Dan Boger
Vicente Garcia

Approved for public release; distribution is unlimited.

19960801 082

DTIC QUALITY INSPECTED 1

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	3. REPORT TYPE AND DATES COVERED
	June 1996	Master's Thesis

4. TITLE AND SUBTITLE: ATTACKING THE INFRASTRUCTURE: EXPLORING POTENTIAL USES OF OFFENSIVE INFORMATION WARFARE

5. FUNDING NUMBERS

6. AUTHOR(S) Elam, Donald E.

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)*

The world has entered the Third Wave; it has entered the Information Age. One of the fundamentals of this paradigm shift is the fact that information is power. The side that controls information more effectively will be victorious. Thus, countries and militaries must change their mentality in order to survive. A new form of conflict, Information Warfare, has been born. This new discipline is large, dynamic, and complex.

The need exists for education among military officers and other concerned professionals throughout the country. This thesis helps to bridge the education gap. It presents a snapshot of Information Warfare today, exploring many different avenues and possibilities along the way. The first half of the document is focused on Information Warfare in general, and the second half deals specifically with the offensive side.

The purpose of this thesis is not to present an all-encompassing view of Offensive Information War or even of Information Warfare in general. The field of Information Warfare is too big for any one individual or organization to fully comprehend all of its intricacies. Indeed, due to the dynamic nature of this discipline, chances are that some, or maybe even all, of the material contained herein will be obsolescent upon publication. The goal of the thesis is to present one view of Information Warfare, as seen through the eyes of many. The hope is that some benefit will be garnered by the reader, even if it only sparks an idea or helps to understand the importance of this growing warfare dimension.

14. SUBJECT TERMS Information Warfare, Information, Warfare, Infrastructure, Offensive, Third Wave			15. NUMBER OF PAGES 216
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18 298-102

Approved for public release; distribution is unlimited.

ATTACKING THE INFRASTRUCTURE: EXPLORING POTENTIAL USES OF OFFENSIVE INFORMATION WARFARE

Donald E. Elam
Lieutenant, United States Navy
B.S., United States Naval Academy, 1990

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
[COMMAND, CONTROL, AND COMMUNICATIONS (C3)]

from the

NAVAL POSTGRADUATE SCHOOL
June 1996

Author: [redacted]
Donald E. Elam

Approved by: [redacted]
Dan Boger, Thesis Co-Advisor

[redacted]
Vicente Garcia, Thesis Co-Advisor

[redacted]
Dan Boger, Chairman
Command, Control, and Communications Academic Group

ABSTRACT

The world has entered the Third Wave; it has entered the Information Age. One of the fundamentals of this paradigm shift is the fact that information is power. The side that controls information most effectively will be victorious. Thus, countries and militaries must change their mentality in order to survive. A new form of conflict, Information Warfare, has been born. This new discipline is large, dynamic, and complex.

The need exists for education among military officers and other concerned professionals throughout the country. This thesis helps to bridge the education gap. It presents a snapshot of Information Warfare today, exploring many different avenues and possibilities along the way. The first half of the document is focused on Information Warfare in general, and the second half deals specifically with the offensive side.

The purpose of this thesis is not to present an all-encompassing view of Offensive Information War or even of Information Warfare in general. The field of Information Warfare is too big for any one individual or organization to fully comprehend all of its intricacies. Indeed, due to the dynamic nature of this discipline, chances are that some, or maybe even all, of the material contained herein will be obsolescent upon publication. The goal of the thesis is to present one view of Information Warfare, as seen through the eyes of many. The hope is that some benefit will be garnered by the reader, even if it only sparks an idea or helps to understand the importance of this growing warfare dimension.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS, ACRONYMS AND/OR ABBREVIATIONS

AFIWC	Air Force Information Warfare Center
AFMC	Air Force Materiel Command
AI	Artificial Intelligence
AIA	Air Intelligence Agency
AMPS	Advanced Mobile Phone System
ASCI	Assistant Chief of Staff for Intelligence
ASAF/AQ	Assistant Secretary of the Air Force for Acquisition
ASD C3I	Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ASSIST	Automated Systems Security and Incident Support Team
ATM	Asynchronous Transfer Mode
AT&T	American Telegraphy & Telephone
B.C.	Before Christ
BDA	Battle Damage Assessment
BDI	Battle Damage Indicators
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control, and Communications
C3I	Command, Control, Communications, and Intelligence
C4	Command, Control, Communications, and Computers
C4I	Command, Control, Communications, Computers, and Intelligence
CDMA	Code Division Multiple Access
CIA	Central Intelligence Agency
CINC	Commander-in-Chief
CISS	Center for Information Systems Security
CJCS	Chairman of the Joint Chiefs of Staff
CNET	Chief of Naval Education and Training
CNN	Cable News Network
COG	Center of Gravity
DBS	Direct Broadcast Satellite
DDCI	Deputy Director for Central Intelligence
DEPSECDEF	Deputy Secretary of Defense
Dept.	Department
DES	Digital Encryption Standard
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency

DIW	Defensive Information Warfare
DOD	Department of Defense
DOS	Denial of Service
e.g.	*exempli gratia* (for example)
e-mail	Electronic Mail
EMP	Electromagnetic Pulse
EPS	Electric Power Simulation
ESC	Electronic Systems Center
ESN	Electronic Serial Number
et. al.	*et alii* (and others)
etc.	*et cetera* (and others)
EW	Electronic Warfare
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDMA	Frequency Division Multiple Access
FEMA	Federal Emergency Management Agency
FIWC	Fleet Information Warfare Center
FLAG	Fiber-optic Link Around the Globe
Gbps	Giga bits per second
GDP	Gross Domestic Product
Ghz	Giga Hertz
GII	Global Information Infrastructure
GOS	Grade of Service
GSM	Global System for Mobile Communications
GW	Giga Watts
HERF	High Energy Radio Frequency
HPM	High Power Microwave
HQMC	Headquarters, United States Marine Corps
IASIW	Institute for the Advanced Study of Information Warfare
Inc.	Incorporated
Info	Information
INMARSAT	International Maritime Satellite
INSCOM	Intelligence and Security Command
Intel	Intelligence
IO	Information Operations
IP	Internet Protocol
IRS	Internal Revenue Service
ISC	Information Systems Command

ISDN	Integrated Services Data Network
iss.	Issue
IW	Information Warfare
IWEB	Information Warfare Executive Board
IWST	Information Warfare Support Team
IXC	Interexchange Channel
JCS	Joint Chiefs of Staff
JFC	Joint Force Commander
JTF	Joint Task Force
kbps	Kilo bits per second
km	Kilometer
LAN	Local Area Network
LED	Light Emitting Diode
LEO	Low Earth Orbit
LIWA	Land Information Warfare Activity
LOAC	Law of Armed Conflict
Mbps	Mega bits per second
MIN	Mobile Identification Number
MOE	Measure of Effectiveness
MOP	Memorandum of Policy
Nat'l	National
NAVSECGRU	Naval Security Group
NCA	National Command Authority
NDC	Naval Doctrine Command
NDU	National Defense University
NII	National Information Infrastructure
no.	Number
NSA	National Security Agency
NSC	National Security Council
OASD C3I	Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence
ODCSINT	Office of the Deputy Chief of Staff for Intelligence
ODCSOPS	Office for the Deputy Chief of Staff for Operations
ODISC4	Office of the Director of Information Systems for C4
OIW	Offensive Information Warfare
OPDEC	Operational Deception
OPSEC	Operational Security

OSD	Office of the Secretary of Defense
OSD NA	Office of the Secretary of Defense for Net Assessment
OSI	Open Systems Interconnection
PCS	Personal Communications Services
PEM	Privacy Enhanced Mail
PGM	Precision Guided Munition
PGP	Pretty Good Privacy
PIG	Personal Interest Group
PKCS	Public Key Cryptography Standard
PSN	Public Switched Network
PSYCOM	Psychological Operations Command
PSYOPS	Psychological Operations
RSA	Rivest, Shamir, and Adleman
SARDA	Assistant Secretary of the Army (Research/Development/ Acquisition)
SC	Assistant Chief of Staff for C4
Sec.	Security
SECDEF	Secretary of Defense
SHF	Super High Frequency
SIGINT	Signals Intelligence
SMDS	Switched Multimegabit Data Service
S/MIME	Secure Multimedia Internet Mail Extensions
SOCCOM	Special Operations Command
SONET	Synchronous Optical Network
SPACECOM	Space Command
SSD	Shared Secret Data
STOD	Special Technical Operations Division
TDMA	Time Division Multiple Access
TRADOC	Training and Doctrine Command
TRANSCOM	Transportation Command
UN	United Nations
U.S.	United States
USA	United States Army
USAF	United States Air Force
USDP IPD	Under Secretary of Defense for Policy Infrastructure Policy Directorate
USMC	United States Marine Corps
USN	United States Navy

USSR	Union of Soviet Socialist Republics
VCNO	Vice Chief of Naval Operations
VGC	Voice Grade Circuit/Voice Grade Channel
VJCS	Vice Chairman of the Joint Chiefs of Staff
vol.	Volume
VR	Virtual Reality
VSAT	Very Small Aperture Terminal
VTC	Video Teleconferencing
WAN	Wide Area Network
XO	Deputy Chief of Staff for Operations
XOX	Doctrine Branch

ACKNOWLEDGMENT

I would like to thank the many people and organizations that contributed to this thesis. Without their support, the journey would have been much more difficult. Many thanks are also due to Dan Boger and Vicente Garcia, true believers in the Third Wave whose patience and guidance were indispensable. Finally, I would like to thank my wife, Joanna, and my sons, Matthew and Christopher, for their support and understanding throughout the whole ordeal.

EXECUTIVE SUMMARY

The world has entered the Third Wave; it has entered the Information Age. One of the fundamentals of this paradigm shift is the fact that information is power. The side that controls information more effectively will be victorious. Thus, countries and militaries must change their mentality in order to survive. A new form of conflict, Information Warfare, has been born. This new discipline is large, dynamic, and complex.

In keeping with this ongoing revolution, the need exists for education among military officers and other concerned professionals througout the country. This thesis helps to bridge the education gap. It presents a shapshot of Information Warfare today, exploring many different avenues and possibilities along the way. Roughly the first half of the document is focused on Information Warfare in general. The second half deals specifically with Offensive Information Warfare.

Like it or not, Information Warfare is a reality today. It is not a fad that will disappear in a few years (or even in the foreseeable future). In its most basic form, Information Warfare has been around for a long time. Technology has been one of the major driving factors in the current paradigm shift to the Information Age. Understanding the enemy's cognitive process and infrastructure are essential for effective employment of Information Warfare as a weapon. These are the major points of Chapter I. Most will be visited again in more detail in later chapters.

Chapter II concentrates on definitions related to Information Warfare. This is perhaps the area of most concern and dissension. Fundamental to a successful manipulation of any weapon is understanding it. Part of the process of understanding that weapon is knowing its language.

There are any number of interpretations of the IW language, and this fact only complicates the problem further.

Chapter III addresses the people, places, and things of IW. It talks about the players involved in the process, from the Executive Branch to the Department of Defense (DOD) to commercial entities. While not every possible organization can be addressed, the reader should be able to get a good feel for the scope and breadth of efforts.

The next chapter, Chapter IV, discusses the role of technology in IW. The rapid technological explosion, with no apparent end in sight, contributes significantly to the potential of Information Warfare. Not only are some of the technologies themselves reviewed, but also the execution of the paradigm shift, in the form of such things as the Global Information Infrastructure (GII), is scrutinized. Finally, the chapter concludes with an examination of some of the current trends in the IW field.

While the first four chapters concentrate mostly on essential background material, Chapter V begins to delve into the major focus of this thesis: Offensive Information Warfare (OIW). The basic definition of OIW, first presented in Chapter II, is reviewed and expanded. Potential reasons that would provoke the use of OIW are explored. Some tools that could be used for OIW attacks are discussed.

Chapters VI forms the heart of the thesis. Up to this point in the thesis, periodic references have been made to the important role of a country's infrastructure in determining the outcome of a conflict. The chapter defines a generic infrastructure that is necessarily broad in scope yet useful for any number of situations. The discussion includes some specifics in using

the template. Various levels of employing OIW against the template are discussed. These levels range from force structures to time lines to Measures of Effectiveness (MOEs).

Chapter VII is a critical review of the difficult issues surrounding the use of OIW. Included in the discussion are political, legal, economic, and moral dilemmas. Other problems discussed include military considerations, repercussions, and coalition OIW operations. For example, how does one coordinate an OIW attack with an ally that may one day be an enemy?

Finally, Chapter VIII presents a review of the thesis and some recommendations on IW for the United States. Included are discussions on definitions, organizations, weapons and tactics, and issues. As IW endeavors increase, so will the number of problems. Only by tackling the hardest issues head-on will one begin to see a decrease in confusion and an increase in productivity. This is by no means an easy task, yet one that is essential to success.

The purpose of this thesis is not to present an all-encompassing view of Offensive Information War or even of Information Warfare in general. The field of Information Warfare is too big for any one individual or organization to fully comprehend all of its intricacies. That is not the purpose of this thesis. Indeed, due to the dynamic nature of this discipline, chances are that some, or maybe even all, of the material contained herein will be obsolescent upon publication. Instead, the goal of the thesis is to present one view of Information Warfare, as seen through the eyes of many. The hope is that some benefit will be garnered by the reader, even if it only sparks an idea or helps to understand the importance of this rapidly growing warfare dimension.

I. INTRODUCTION

A. THE CHANGING FACE OF WARFARE

Information has played a significant role in determining the outcome of armed conflict throughout history. Starting with the Punic Wars and continuing to the high-tech wars of the 1990's, information has been a critical factor. In almost every major historical period, at least one example can be found. For brevity's sake, only a few of the more celebrated examples will be reviewed.

Perhaps the earliest recorded use of decisive information exploitation occurred in the second century B.C. with Hannibal during the Second Punic War. Hannibal maintained a series of hilltop sentries armed with mirrors who would relay information concerning Roman troop movements to him. Such superior knowledge of the enemy gave Hannibal a decisive edge for many years. In fact, it helped him to defeat a Roman army twice the size of his at the Battle of Lake Trasimene.[Ref. 1]

One of the most successful early users of information were the Mongol hordes in the 13th century. They employed "arrow riders"[1] for swift communications across large distances. This allowed Mongol commanders to be well-informed about enemy movements. Furthermore, they intercepted enemy scouts and prevented them from reporting. As a result, Muslim commanders were blind. The Mongols used this to their advantage and enjoyed numerous successes on the

[1] Arrow riders are roughly analogous to the Pony Express of the 19th century United States.

battlefield, most notably during the Khwarizm campaign. Although superior communication was not the only factor for the Mongols' success, it was a significant one.[Ref. 1]

Effective use of information continued to abound throughout history. American Revolutionary War hero General George Rogers Clark exploited information in the form of deception, coupled with sniping of British sentries, to induce a surrender to his numerically inferior force. British naval captain Lord Cochrane used information to confuse and dominate the French coastline in 1798[Ref. 1]. The invention of new communication systems, such as the telegraph and the radio played increasingly important roles in warfare throughout the nineteenth and early twentieth centuries. World War II saw a significant advance in the importance of information in warfare, mainly due to technological advances. Innovations such as radar played a significant role in early warning. Codebreaking initiatives such as Ultra and Magic gave the allies a decisive edge.[Ref. 2] More and more, the side that had the better information had the advantage.

Perhaps the most touted example of recent effective information exploitation occurred during Operation Desert Storm. Coalition forces targeted Saddam Hussein's Command, Control, Communications, Computers, and Intelligence (C4I) nodes. This left Iraqi forces virtually blind. At the same time, the coalition pooled its own C4I resources to ensure their commanders constantly had the best possible battlefield picture.[Ref. 3] Soviet Lieutenant General Bogdanov, Chief of the General Staff Center for Operational and Strategic Studies, commented shortly after Desert Storm,

> Iraq lost the war before it even began. This was a war of intelligence, EW [Electronic Warfare], command and control and counter intelligence. Iraqi troops were blinded and deafened...Modern war can be won by *informatika*[2] and that is now vital for both the U.S. and USSR.[Ref. 4]

Although the use of information has generally taken a backseat to the physical application of force in determining the outcome of a conflict, wars of the future will be unlike any we have seen in the past. Desert Storm proved that. In the wake of that conflict, people began to realize *en masse* that a dynamic shift in traditional warfighting was underway. In fact, early rumblings occurred almost 15 years earlier when a Russian officer named Ogarkov foresaw this change. He espoused a changing theory of warfare whereby increasingly mobile communications would encompass a larger theater of war with a decreased timeline.[Ref. 5] Such is the trend today.

B. THE CHANGING PARADIGM

1. The Future of Warfare

Imagine the battlefield of the future (it is in fact, not really a field at all, but rather an Nth-dimensional "battlespace"). Nation X is in dire straits. People are starving in the harsh winter, the economy is in shambles, and discontent is everywhere. The only thing Nation X's dictatorial government has to bargain with are nuclear weapons. Nation X demands that the prosperous Nation Y immediately send food and financial aid or face the wrath of nuclear holocaust. The United Nations (UN) invokes sanctions on Nation X while calling for disarmament of their nuclear weapons and compliance with international treaties.

Undaunted by Nation X's threats, a small team of Nation Y's experts sit down in front of their computer terminals. They penetrate Nation X's computers and begin working their magic.

---

[2] Roughly translates from Russian to 'Information Warfare'.

First, the computers that control Nation X's nuclear weapons cease to work, for no apparent reason. Then, all over Nation X, strange things begin happening. Electric power grids suddenly shutdown for no reason and come back up minutes later on their own. Central phone system computers go berserk. The financial institutions see their funds and assets disappear, only to reappear 30 minutes later. At natural gas switching stations around the country, operators lose control of the system. On computer monitors across the country, the following message appears, "You are in violation of U.N. resolution 1234. Acquiesce immediately or suffer the consequences."

Concurrently, Nation Y covertly airdrops thousands of tiny sensors across Nation X. These sensors interconnect and immediately begin transmitting information. In short order, Nation Y knows exactly how Nation X's conventional forces are deployed. The sensors begin jamming Nation X's military and commercial communications. Nation X's forces cannot communicate and are rendered virtually powerless.[3][Ref. 6]

Reluctantly, Nation X ceases its belligerence. United Nations' teams enter the country and begin the process of nuclear disarmament. Nation X revolts and ousts its dictator, setting in his place a freely elected president. The world is safe once again. Nation Y has averted global holocaust with no lives lost.

The above scenario is but one example of future warfare. This type of warfare need not be focused around large armies or weapons of mass destruction. In fact, this type of warfare need

[3] This is an example of the Mesh Theory as advocated by Martin Libicki of the National Defense University.

not incur any human fatalities. This type of warfare is unbounded. It can happen anywhere, anytime, at any level of intensity. This is the future of warfare.

2. The Third Wave

What has led to this type of warfare? The answer is complex, and there are a large number of reasons for this complexity. Perhaps the easiest way to explain this change is to say that a major paradigm shift has taken place. The world has entered the Third Wave; it has entered the Information Age. The First Wave was an agricultural society. The Second Wave was an industrial society. The Third Wave is an information society. At each paradigm shift, major changes in warfighting have taken place. As the world enters the Third Wave, information is power. The side that controls information most effectively will be victorious.[Ref. 7]

Based on these radical changes ongoing across the world in all facets of society in conjunction with the paradigm shift, a new type of warfare needs to be defined, molded, and applied when necessary. That new classification is called Information Warfare (IW). Throughout the rest of this chapter, the term "Information Warfare" will be used freely. No formal attempts will be made to define it until the next chapter. This apparent oversight is intentional. It is meant to provoke the reader to think, in his or her own mind, "What is Information War?" This nebulous question is a very controversial and current topic, and it is the focus of Chapter II. One should also note that IW embraces or includes any number of additional terms, such as Information-Based Warfare, Cyberwar, Netwar, Hacker Warfare, etc.; each of these terms (and many more) will be discussed in detail in the following chapter.

C. WARFARE THEORY

The study of warfare is a discipline and a science onto itself. Numerous tomes and dissertations have been written on the theoretical ways that warfare should be waged. These writings range anywhere from the scientific to the intuitive. They have formed the core of military leadership training for generations. Despite the radical paradigm shift in warfare that is ongoing, there is still room for some of the classic works.

1. Traditional Views of Warfare

Several of the "great classic thinkers" of warfare theory wrote about Information Warfare without calling it such. In each case, the role of information was emphasized as a decisive factor in waging war. To make the point, the works of two such thinkers, Sun Tzu and Clausewitz, will be examined.

One of the greatest military thinkers ever was Sun Tzu, an extremely foresighted general in ancient China. The fact that his thoughts are still largely applicable 23 centuries later is a testament to the power of his work. One of his best known quotes is "Know the enemy and know yourself; in a hundred battles, you will never be defeated".[Ref. 8] The implication of information dominance is clear. Although the actual execution of warfare is radically different today, the basic premise remains the same. One has already seen uses of information exploitation throughout history. Third Wave thinking only accentuates Sun Tzu's words.

A second example can be found in the works of Clausewitz, a Prussian military strategist of the 19th century. He defined information as "the foundation of all of our ideas and actions".[Ref. 9] Most of his discourse on information is spent talking about how information can be corrupted, how the commander should be wary of all information, etc. Yet the power of

his argument can be a modern interpretation of the above quote; information forms the foundation upon which all of a military commander's decisions rest. If one can break this foundation, the commander is powerless. At the same time, that commander must take steps to protect the foundation. Protecting and destroying or manipulating that foundation is one example of Information Warfare. Defining exactly what that foundation is and how to break it is one of the primary focuses of this thesis.

2. Role of Technology in Warfare

By now, one can see the importance that information plays in warfare. One should also see another common thread: the increasing importance of information in warfare runs parallel to advances in technology. Martin Van Creveld, a noted historian and respected author, preaches the importance of technology in warfare:

> [W]ar is completely permeated by technology and governed by it. The causes that lead to wars, and the goals for which they are fought; the blows with which campaigns open, and the victories with which they (sometimes) end; the relationship between the armed forces and the societies that they serve; planning, preparation, execution, and evaluation;...even the very conceptual frameworks employed by our brains in order to think about war and its conduct--not one of these is immune to the impact that technology has had and does have and will have.[Ref. 10]

This is a powerful statement about the role of technology in warfare. Technology plays a role in every facet of warfare and always will. Technology has been one of the major contributors (if not the major contributor) in the transition to the Information Age. Technology is the driving force of Information Warfare just as Information Warfare is a slave to technology. The two cannot be separated; one must understand the state of technology in order to effectively

understand Information Warfare. Throughout this thesis, the role of technology will continuously be addressed. It is also the focus of Chapter IV.

3. Importance of the Cultural Dimension

As seen earlier in the Clausewitz discussion, exposing the enemy's information foundation is the crux of Information Warfare. Sun Tzu stressed "knowing your enemy as yourself"[Ref. 8]. This involves getting inside the enemy's thought process. It means understanding how the enemy thinks. This is no easy task. People think differently. A substantial part of understanding an enemy's thinking is to understand his environment. Different regions of the world have different beliefs, customs, and environments, and thus they have different thought processes. The effective commander will understand his counterpart's environment and how it can be manipulated to his advantage.

Information Warfare is no different, and, in fact, can be more challenging. For example, a potential hostile nation may configure its telecommunications network in a seemingly senseless manner. If one is going to penetrate that network, one needs to understand the rationale behind the network's structure. Only then can it be exploited in an optimal fashion. This is one of the greatest (and most important) challenges facing those who would wage Information Warfare.

4. Center of Gravity

Carrying the Clausewitz argument one step further, the information foundation can be viewed as an infrastructure[4]. While not elaborating on the organization of this infrastructure, one can say that attempts to break this foundation are attempts to destroy Centers of Gravity(COGS).

---

[4] The exact definition of "infrastructure" in the context of this thesis is the focus of Chapter VI.

Joint Publication 0-1 defines Center of Gravity as "[t]hat characteristic, capability, or locality from which a military force, nation, or alliance derives its freedom of action, physical strength, or will to fight. It exists at the strategic, operational, and tactical levels of war".[Ref 11] Thus, in order to effectively use Information Warfare against an enemy's infrastructure, one must understand where the Centers of Gravity lie. They are the weak links that can be exploited.

D. THE IMPORTANCE OF INFORMATION WARFARE

The burgeoning field of Information Warfare presents new opportunities as well as potentially deadly traps for the military commander. Warfare can now be waged in seconds across thousands of miles with no loss of life while leaving little trace of the attacker. Yet, effective employment of IW involves a radical shift in traditional thinking (not always an easy task, but an essential one in this case). As the transition to the Information Age becomes more pronounced, new methods must be devised to defeat old enemies and new protections created to defend old systems. Some actions are already underway in these areas. These efforts need to be intensified. This thesis hopes to offer insight into possible ways of accomplishing some of these tasks.

E. FRAMEWORK FOR INFORMATION WARFARE AS A WEAPON

Like it or not, Information Warfare is a reality today. It is not a fad that will disappear in a few years (or even in the foreseeable future). In its most basic form, Information Warfare has been around for a long time. Technology has been one of the major driving factors in the current paradigm shift to the Information Age. Understanding the enemy's cognitive process and infrastructure are essential for effective employment of Information Warfare as a weapon. These are the major points of Chapter I. Most will be visited again in more detail in later chapters.

Chapter II concentrates on definitions related to Information Warfare. This is perhaps the area of most concern and dissension. Fundamental to a successful manipulation of any weapon is understanding it. Part of the process of understanding that weapon is knowing its language. There are any number of interpretations of the IW language, and this fact only complicates the problem further.

Chapter III addresses the people, places, and things of IW. It talks about the players involved in the process, from the Executive Branch to the Department of Defense (DOD) to commercial entities. While not every possible organization can be addressed, the reader should be able to get a good feel for the scope and breadth of efforts.

The next chapter, Chapter IV, discusses the role of technology in IW. The rapid technological explosion, with no apparent end in sight, contributes significantly to the potential of Information Warfare. Not only are some of the technologies themselves reviewed, but also the execution of the paradigm shift, in the form of such things as the Global Information Infrastructure (GII), is scrutinized. Finally, the chapter conncludes with an examination of some of the current trends in the IW field.

While the first four chapters concentrate mostly on essential background material, Chapter V begins to delve into the major focus of this thesis: Offensive Information Warfare (OIW). The basic definition of OIW, first presented in Chapter II, is reviewed and expanded. Potential reasons that would provoke the use of OIW are explored. Some tools that could be used for OIW attacks are discussed.

Chapters VI forms the heart of the thesis. Up to this point in the thesis, periodic references have been made to the important role of a country's infrastructure in determining the

outcome of a conflict. The chapter defines a generic infrastructure that is necessarily broad in scope yet useful for any number of situations. The discussion includes some specifics in using the template. Various levels of employing OIW against the template are discussed. These levels range from force structures to time lines to Measures of Effectiveness (MOEs).

Chapter VII is a critical review of the difficult issues surrounding the use of OIW. Included in the discussion are political, legal, economic, and moral dilemmas. Other problems discussed include military considerations, repercussions, and coalition OIW operations. For example, how does one coordinate an OIW attack with an ally that may one day be an enemy?

Finally, Chapter VIII presents a review of the thesis and some recommendations on IW for the United States. Included are discussions on definitions, organizations, weapons and tactics, and issues. As IW endeavors increase, so will the number of problems. Only by tackling the hardest issues head-on will one begin to see a decrease in confusion and an increase in productivity. This is by no means an easy task, yet one that is essential to success.

The purpose of this thesis is not to present an all-encompassing view of Offensive Information War or even of Information Warfare in general. The field of Information Warfare is too big for any one individual or organization to fully comprehend all of its intricacies. That is not the purpose of this thesis. Indeed, due to the dynamic nature of this discipline, chances are that some, or maybe even all, of the material contained herein will be obsolescent upon publication. Instead, the goal of the thesis is to present one view of Information Warfare, as seen through the eyes of many. The hope is that some benefit will be garnered by the reader, even if it only sparks an idea or helps to understand the importance of this rapidly growing warfare dimension.

II. DEFINING INFORMATION WARFARE

A. WHAT IS INFORMATION WARFARE?

Defining Information Warfare (IW) is a very complex task, perhaps an impossible one. There are any number of different views and perspectives. These various arguments can get very complicated, very quickly. They range from the very basic and trite (so that the average man or woman on the street can understand) to the very profound and philosophical (introducing such higher thinking concepts as Complexity Theory, Decision Theory, Utility Methods, etc.).

The goal of this chapter is to expose the reader to some of the many different perspectives and definitions in the field of Information Warfare. Therefore, various definitions and views of the subject will be presented from a wide variety of entities. At first, this approach may seem confusing, monotonous, and perhaps not very useful. However, the goal is not to have the reader memorize a bunch of definitions, but rather it is to show the reader how large and diverse the discipline of Information Warfare really is. At the same time, some common trends and mistakes can be seen that can be used to form a common view, although not a perfect definition.

Perhaps the greatest challenge facing the players in the Information Warfare realm is definitions. In fact, defining Information Warfare is one of the hottest items in government circles today. Everyone is trying to define IW in their own unique way. Why? What is so important about definitions? Some would argue that definitions are not really important. If the main sticking point is definitions, push them aside and get to something more tangible and productive. The author would argue definitions are important. Only when organizations are speaking a common language (as defined by common terms and definitions) is full efficiency

reached. At the same time, one should realize that such utopian ideas are not achievable in today's world. Still, some commonality could and should be reached. As shall be seen, there exists today any number of different views that need to be consolidated. Although the various entities involved in IW are mostly talking, individual goals and organizational "rice bowls" need to be set aside if any real progress is to be made.

B. TYPES OF INFORMATION WARFARE

Table 1 is a sample of just a few of the many terms that are used to describe essentially the same thing (what has just been called "Information Warfare" so far).

Information Operations	Command & Control Warfare	Information In War
Information-Based Warfare	Electronic Warfare	Neocortical Warfare
Syntactical Warfare	*Informatika*	Semantic Warfare
Cyberwar	Computational Mobile Warfare	Low-Intensity Warfare
Netwar	Decision Cycle Warfare	Hacker Warfare
Cognitive Warfare	Fuzzy Logic Warfare	Cybernetic Warfare
Cyberspace War	Soft War	Reflexive Control
Epistemological Warfare	Computer Warfare	Just-In-Time Warfare

Table 1. Various Terms Relating To Information Warfare.

Some of these terms will be explored in more detail below while others will never again be mentioned. The idea is to show the reader there are many terms that relate to the same basic concept.

1. Selected examples of different views

The following paragraphs are a series of quotations and paraphrases that outline some of the many different interpretations of Information Warfare that exist today.

a. National Level Decision Makers

The importance of Information Warfare is realized at the highest levels of the U.S. government. The Honorable Newt Gingrich, Speaker of the House, is a renowned advocate of Information Warfare. He has made numerous public appearances on the subject and even introduced legislation related to it. His definition of Information Warfare is "the use of information to achieve your purposes".[Ref. 12] This a very broad definition and could be interpreted any number of ways. Therefore, it is not very useful, but the point is that top government officials are aware of IW and its significance.

Also, this definition shows the beginning of a recurring theme: the use of the word "information" in the definition. A grammatical rule of thumb states that when defining a word, one should never use that word. By doing so in this case adds a whole new level of complexity to the problem. By not defining information (which in itself can be defined any number of ways), more questions are introduced. The difficulty of a useful definition grows quickly.

b. Department of Defense

The Department of Defense is perhaps one of the most important players involved in the Information Warfare world. Yet there are difficulties in defining the term. At the highest levels in the department, there exist no less than two definitions for IW.

The Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD C3I) defines Information Warfare as "actions taken to achieve information superiority in support of national military strategy by affecting adversary information systems while leveraging and protecting our information and information systems".[Ref. 13] This definition offers more substance than Mr. Gingrich's and might be useful

if the word "information" did not appear in the definition four times. Also, a new problem is introduced. What is meant by the terms "information superiority", "information systems", and "leveraging"? One can see that such a definition cannot stand on its own; rather, associated terms must also be defined.

Another definition from the Department of Defense (DOD) can be found in the draft revision of DOD Directive 3600.1. Although this is only a draft and should not be taken as official policy, it can be used to illustrate a point. The original 3600.1 was a highly classified document that could not be seen by very many people and thus was not very useful. The new revision will be somewhat less classified and offers this unclassified definition: "actions taken to achieve information superiority by affecting adversary information, information systems, and information processes while defending one's own information, information systems, and information-based processes".[Ref. 14] This definition is only slightly different than the previous one and offers the same kinds of problems ("information" is used seven times, "information-based processes" are unclear, etc.). This definition also tends to contradict the other one somewhat. Although this definition comes from a draft and should not be taken as final, it is being circulated in official briefings. This only leads to more confusion and could possibly discredit the organization involved (*e.g.,* why is this organization using two conflicting definitions for the same term?).

The Army prefers to use the term "Information Operations" which it defines as

> continuous military operations within the military information environment that enable, enhance, and protect the commander's decision cycle and mission execution to achieve an information advantage across the full range of military operations. Information Operations include interacting with the global information

> environment and, as required, exploiting or degrading an adversary's information and decision systems.[Ref. 15]

They then define Information Warfare using a proposed definition from Joint Publication 1-02 (DOD Dictionary of Military and Associated Terms). This definition is very similar to the DOD definitions above. In the Army's view, IW is a subset of Information Operations (IO) and IW is implemented by employing Command and Control Warfare (C2W). C2W is discussed in detail later in this chapter.

The Navy has formally endorsed Information Warfare. They define IW as

> action taken in support of national security strategy to rapidly seize the initiative and maintain a decisive information by attacking an adversary's information infrastructure through exploitation, denial, and influence, while protecting friendly information systems.[Ref. 16]

This has often been reduced by Navy briefers to the three major points of Exploit, Protect, and Attack. Again, one can see that the word "information" appears three times and other questions are raised (*e.g.*, what is an "information infrastructure"?). Furthermore, official Navy policy documents (*e.g.*, OPNAVINST 3430) often erroneously equate IW to C2W by writing "IW/C2W". Later discussion will show that while the two are related, they are not equal.

The Air Force defines Information Warfare as "any action to deny, exploit, corrupt, or destroy the enemy's information and its functions; protecting ourselves against those actions; and exploiting our own military information functions."[Ref. 17] IW is further broken down into Psychological Operations, Electronic Warfare, Military Deception, Physical Destruction, Security Measures, and Information Attack. If one were to overlook the use of "information" in the definition, this perhaps is a good definition. Yet, the Air Force's idea of IW execution (in the form of the six principles listed above), contains all of the pillars of C2W

(described later) and only one "new" aspect: Information Attack. One might thus imply the Air Force views IW as enhanced C2W.

To date, the Marine Corps has not formally embraced the idea of Information Warfare. Although they realize the importance of information, their perspective centers almost entirely on C2W. One could say that the Marine Corps is wisely biding their time until everyone else figures out what IW is and how the military can use it.

c. Academic Experts

As might be expected in any new innovation in warfare, the military's academic support community has been involved in the Information Warfare definition debate. Most notably, the National Defense University (NDU)'s staff has published several different views on IW. Perhaps the most concise document is their dictionary of IW-related terms. Although this is a very comprehensive manuscript, it clearly (although not directly) states the problem. It contains four different definitions for Information-Based Warfare (the preferred NDU term) and two definitions of Information Warfare.[Ref. 18]

Martin Libicki of NDU fully realizes the problem. He refers to the various attempts to define Information Warfare by using the analogy of the blind men and the elephant. The blind men are all around the elephant, trying to figure what it is. Each can only touch a certain part so each offers a different definition on what the creature is. Such is the case in the IW definition fiasco; the various players have blinded themselves and are only seeing a small part of a larger beast. Mr. Libicki's argument is not unique; many people have used the same analogy because it so aptly describes the severity of the problem in defining Information Warfare. Mr Libicki thus, perhaps wisely, never tries to define IW. Instead, he offers seven different

components that comprise it.[Ref. 19] These views, along with their various sub-components, are shown below in Table 2.

COMPONENT	SUB-COMPONENT	COMPONENT	SUB-COMPONENT
C2W	Anti-head	Psychological Warfare	Anti-will
	Anti-neck		Anti-troop
Intelligence-Based Warfare	Offensive		Anti-commander
	Defensive		*Kulturkampf*
Electronic Warfare (EW)	Anti-radar	Cyberwarfare	Info-terrorism
	Anti-comms		Semantic
	Cryptography		Simula-warfare
Economic IW	Econ. Blockade		Gibson-warfare
	Techno-Imperialism	Hacker Warfare	None

Table 2. Martin Libicki's View of Information Warfare.[After Ref. 19]

A detailed explanation of each of the terms in Table 2 is not necessary in the context of this discussion. Some of them will be looked at in further detail in later chapters. For more information or further clarification, the reader should refer to Martin Libicki's book, *What Is Information Warfare?* The main point here is that IW covers a lot of different things, some of which fall under traditional military missions (C2W, EW, etc.) while others are new (*e.g.*, Hacker Warfare).

d. The Experts

No discussion of Information Warfare definitions and perspectives would be complete without offering some insight from the "experts" in the field of IW. These renowned thinkers were among the pioneers that brought to light the importance of Information Warfare.

Of course, the examples presented here are but a small part of the many "expert" viewpoints that exist.

John Arquilla and Dave Ronfeldt offer yet another view of Information Warfare in a 1993 RAND report. They espouse the terms "Cyberwar" and "Netwar" in lieu of Information Warfare. Cyberwar is the broad term that "refers to conducting military operations according to information-related principles."[Ref. 20] It builds upon traditional warfare missions and brings them into a new focus that is primarily technology-based. Netwar is basically the same kind of things but focused at the strategic level between nations (whereas Cyberwar is more operational and tactical in nature). These two terms offer a good starting point for definitions, but they are too broad to be of much effective use in coming to grips with a concise definition.

Winn Schwartau has often been credited with raising public awareness about the importance of Information Warfare in his book *Information Warfare: Chaos On The Electronic Superhighway.* While some of his statements of fact are in reality just science fiction (for the moment at least), he has some good ideas to offer. His definition of IW is "an electronic conflict in which information is a strategic asset worthy of conquest or destruction." [Ref. 21] The strength of this definition is the realization that information is a "strategic asset."

Retired Air Force Colonel Al Campen offers a very good, but not perfect, definition of Information Warfare:

> A political, economic, or war strategy, to achieve a competitive advantage by attacking adversary information systems, while protecting your own. The goal is to achieve a knowledge differential by limiting the quality and quantity of information available to a competitor.
> [Ref. 22]

This definition, while using the terms "information" and "knowledge", shows that IW includes

more than just purely military aspects (much as Martin Libicki's view did earlier in this chapter).

George Stein of the Air University builds on the ideas of others and offers his insight into how those ideas might be employed effectively. While he realizes Information Warfare spans a wide variety of fields, he also offers that IW also occurs at each of the traditional warfare levels: Strategic, Operational, and Tactical.[Ref. 23] Although this idea was alluded to in the Arquilla/Ronfeldt discussion earlier, further clarification of this important concept is necessary because it adds a whole layer of complexity to the definition problem. Not only does Information Warfare occur horizontally across a wide range of fields, it also occurs vertically at varying degrees of intensity and focus.

e. Miscellaneous Entities

Even "amateur" thinkers have something useful to offer to the discussion of definitions. Often not driven by organizational politics, they can more easily offer insight without getting too involved in syntax or political correctness. Three such views are offered here as an example of "freer" thinking.

The United States is not the only country that is thinking about Information Warfare (this idea will be revisited in later chapters). In fact, even Canada has realized the power of this emerging discipline. An officer in the Canadian Navy, Lieutenant Garigue, offers his own views of IW: "[IW] consists of all efforts to control, exploit, or deny an adversary's capability to collect, process, store, display, and distribute information, while at the same time preventing the enemy from doing the same."[Ref. 24] Although the word "information" is used in the definition, this is still a good definition in that it tells how the information is to be manipulated (collect, process, store, etc.).

Two other opinions on Information Warfare can be found in two papers on the Internet homepage of the unobtrusive Institute for the Advanced Study of Information Warfare (IASIW). One uses the proposed DODDIR 3600.1 definition (shown above in the discussion of DOD) but breaks IW into three "practical" areas: Personal IW, Corporate IW, and Global IW.[Ref. 25] This broad perspective again shows not only the breadth that IW encompasses but also demonstrates that IW need not be limited to the military or political realm; in fact, IW can be found in the business world as well (which has been alluded to previously but never specifically stated). The second IASIW paper uses more basic terminology by saying "Information Warfare is a war in which the weapons of warfare are not guns and bombs and bullets that visibly destroy flesh, blood, and bone, but [rather use] electronic and electromagnetic weapons..." [Ref. 26] Although this simplistic definition leaves out a lot, it's value is that it is written such that almost anyone can understand it.

2. Information Warfare versus Command and Control Warfare

The relationship of Information Warfare and Command and Control Warfare has been seen in the majority of the cases examined. C2W was a mission of the military before IW became a "hot" topic. The Joint Chiefs of Staff Memorandum of Policy Number 30 (MOP 30) defines five pillars that comprise C2W: Electronic Warfare (EW), Operational Deception (OPDEC), Operational Security (OPSEC), Psychological Operations (PSYOPS), and Physical Destruction.[Ref. 27] One can easily see that most of the definitions examined in this chapter include one or more of these tenets. However, there are many things in the various definitions above that do not fall under any of these five pillars. Conversely, not all five pillars can be applied to IW in all cases. Consequently, IW and C2W are closely related, but they are not

equivalent. The best way to look at C2W is as a sub-component of IW. This sub-component does not necessarily fully overlap the IW domain (*e.g.*, not all Physical Destruction in the C2W realm is IW) and is one in which the military is ideally suited to execute.

C. A CONSOLIDATED VIEW

So what is Information Warfare? The answer is simply that it can be anything and everything, depending on how one defines it. Of course, that is not a very useful definition. At the same time, one must also realize that there is no realistic way to achieve the "perfect" definition.

1. Coming To Grips With A Definition

Still, any discussion of defining IW should avoid certain common pitfalls which have been seen in the various definitions. A partial list of things to avoid include:

- No definition of Information Warfare should include the word "information" in it, unless accompanied by an explanation of what information is in the context of the definition.
- Any additional terms that are used in the definition (*e.g.*, information-based processes) should be defined or explained immediately.
- Definitions should be written in a language understandable to the intended audience.
- Definitions should not be too broad as to encompass everything or too narrow as to leave out critical points.
- Definitions should closely match other organizations' definitions as much as possible.

Paying attention to these shortcomings and avoiding them will enhance any IW definition.

Also, any discussion of IW should also include certain realities which are common to most definitions, as shown below:

- No one definition can stand alone; it must be accompanied by amplifying information.
- Information Warfare is not the same thing as Command and Control Warfare. Rather, C2W is a critical sub-component of IW.
- Information Warfare encompasses a wide range of disciplines. It involves more than just the military. In fact, government, business, industry, politics, economics, and education are some of the other players involved with or that have a stake in IW.
- Information Warfare is found in varying degrees of intensity, at varying levels of conflict, from peace to war and from the strategic level to the tactical level.

Of course, these lists are not meant to be all-inclusive, but instead are meant to serve as reminders to some of the problems facing those attempting to define Information Warfare.

Considering all of the problems that exist with trying to define Information Warfare, a reasonable person might ask: is it possible to define IW in terms that are useful, understandable, and amenable to a common syntax? The realistic answer is: probably not. Then the next question should be: does one need a common, clear, and concise definition? As mentioned in the opening paragraphs of this chapter, the answer to that question is: yes, without a doubt. Well, then what is to be done? If one cannot use words, what can one use?

Perhaps pictures can be used. Pictures reduce the number of words required to define a problem; this increases the chance for agreement amongst the various factions. Also, pictures can more easily depict a complex multi-layered , multi-faceted problem, such as IW. Finally, pictures can be tailored to the audience at hand; the level of complexity and detail can vary with

the user of the picture. Of course, care must be taken to ensure that a fairly uniform interpretation is created by using a standard guide. These steps can provide a powerful definition tool that is flexible and diverse.

2. A Possible Answer: Paradigm F

While accepting the fact that no one picture or series of pictures can totally represent Information Warfare, some are better than others. One of the better series of diagrams is called Paradigm F. Paradigm F is a concept espoused by Dr. Fred Giessler of the National Defense University. Paradigm F consists of five figures (Figures 1 through 5) that are contained on the following pages.[Ref. 28] A tailored view of Paradigm F, coupled with the author's own interpretation, is the main definition of Information Warfare that will be used throughout this thesis. Not all parts of the figures will be discussed at this time. Some will be detailed in subsequent chapters while others will not be used at all.

Figure 1 represents the basic view of Paradigm F. Figure 2 is the same diagram with amplifying details and examples. This "onion skin" diagram shows the layers that define the United States. At the most fundamental level (the outermost layer) is the country's national purpose. Here one finds the ideals upon which the country is built, such as peace and freedom, and outlined in documents such as the Constitution and the Bill of Rights. These ideals form the basis for the next layer which is national interests. This layer contains our national objectives and marks the beginning of our government, starting with the President. From these national interests come the next layer which is the national grand strategy. Here the bureaucracy of the government enters the picture with such entities as Congress.

As the layers continue inward, they build on the preceding outer layers. Also, the migration inward brings with it more details. This can best be seen in the center of the left-hand side. This shows the division of the strategic, operational, and tactical levels of war. Each layer shows examples of the organizations involved (*e.g.*, the Joint Chiefs of Staff are found in the national military strategy layer) as well as traits of that layer (*e.g.*, the national grand strategy layer is characterized by the subdivisions economical, political, cultural, etc.). At first glance, this may appear quite impossible to understand, but after a few minutes of studying it, it becomes almost intuitive.

The thick black line on the right-hand side shows the Information Warfare domain. One should note that this domain cuts across all facets of the paradigm, albeit with varying degrees of influence. The influence is most heavy near the center and extends outward to midway through the operational level of war. Then begins a gradual taper to almost no influence at the outer edge of the strategic level. At the heart of the paradigm is C2W. This represents the lowest level of execution of the outermost layer. One might say that the move inward along the diagram brings with it a decreasing level of theory and an increasing level of tangibility.

While these first two diagrams help one to understand where Information Warfare fits into the larger picture, they do not explain what Information Warfare is. To facilitate this explanation, one needs Figures 3 through 5. Each of the figures is entitled "Paradigm F.1" and is dedicated to the Information Warfare domain. The x-axis of each of the three diagrams shows the spectrum of conflict, from peace to war and back to peace. Underneath that is depicted the national security environment continuum and shows where each of the Combatant Commanders (CINCs) and Joint Force Commander (JFCs) are involved (one should notice that the CINC is

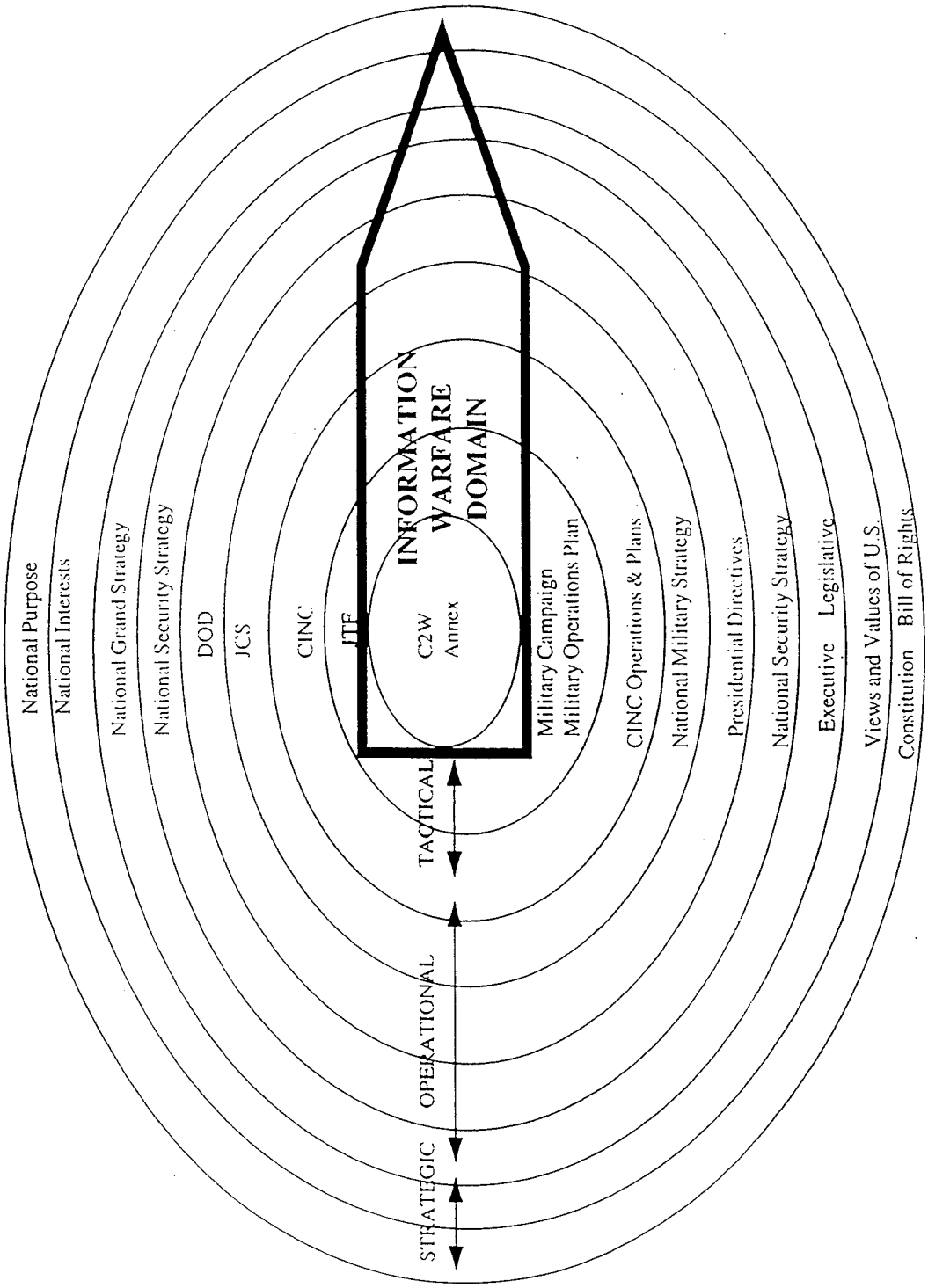

Figure 1. Paradigm F (1 of 2).[From Ref. 28]

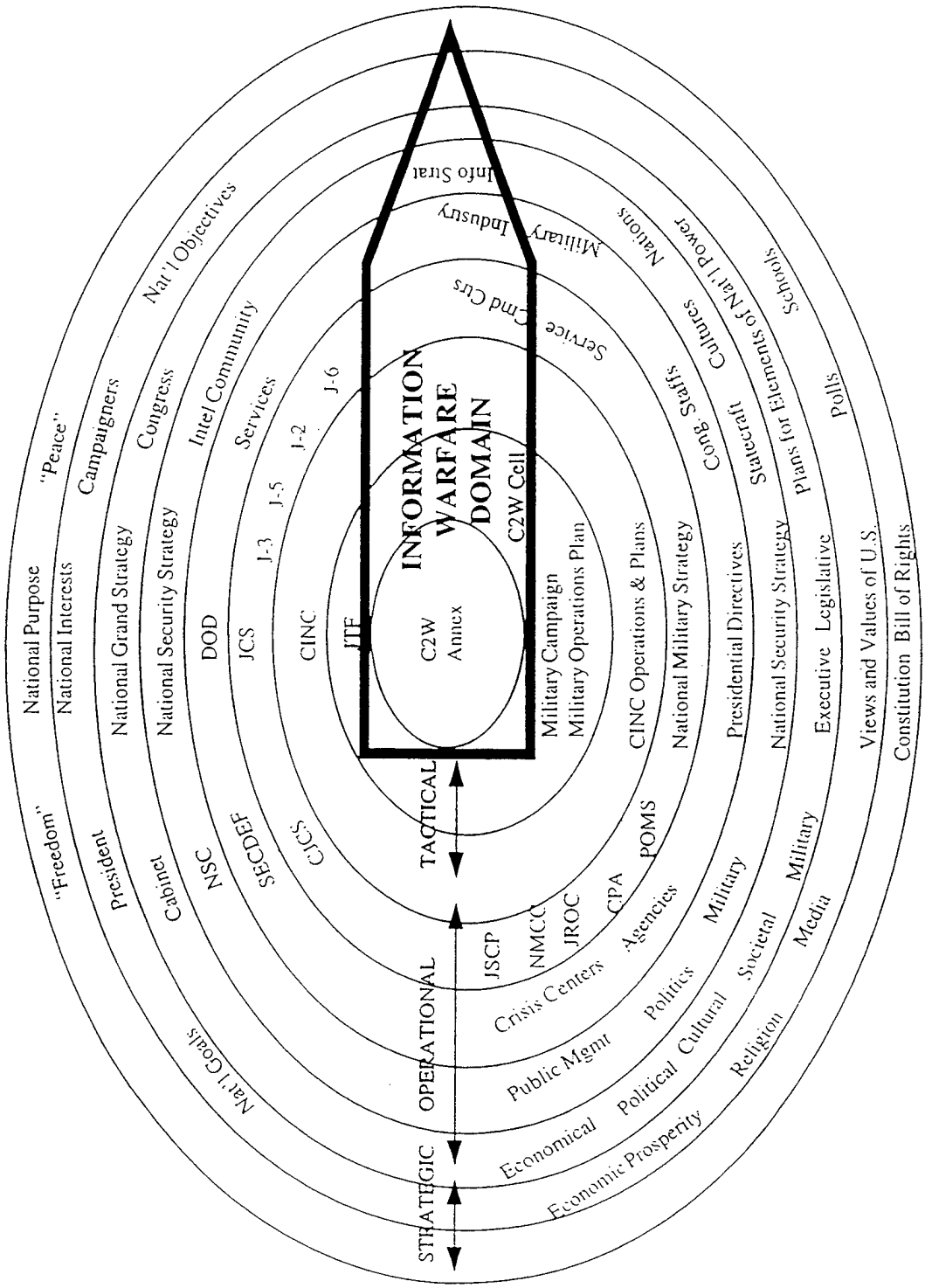

Figure 2. Paradigm F (2 of 2).[From Ref. 28]

involved almost throughout). The y-axis of each diagram shows the non-linear quantity of effort required for the elements of the curves.

Each of the three figures has two curves (they are the same on all three); the upper curve represents Information Warfare while the lower curve shows C2W. Figure 3 provides details for C2W. The various elements that comprise C2W are listed under the curve. The arrows represent the range of the national security environment where those elements apply. The height of those arrows are the amount of effort required to execute those elements. Notice such things as Command, Control, Communications, Computers, and Intelligence (C4I) require very little relative effort and span the entire continuum while C2 Destruct occurs only around war and requires a lot of effort. Definitions for each of the elements on the diagrams are not important for the context of this chapter. Some of the elements will be revisited in greater detail in later chapters.

Figure 4 displays the details of the Information Warfare curve. The smaller text on the right-hand side shows the different focus areas of Information Warfare: military, energy, leadership, religion, society, governance, and political power. More importantly (for later chapters), this small text also lists some of the major centers of gravity (education, banking, media, transportation, telecommunications, customs, etc.). The larger text on the left-hand side shows a list of some of the more specific ways that IW can be implemented (*e.g.*, manage perceptions, sever-degrade C2/C3/C4I, etc.). This list is, of course, not all-inclusive. The height of the text again shows the relative amount of effort required to accomplish that task. Finally, Figure 5 is merely a combination of Figures 3 and 4. It shows both the Information Warfare curve and the C2W curve. Together, they represent the IW domain shown on Figures 1 and 2.

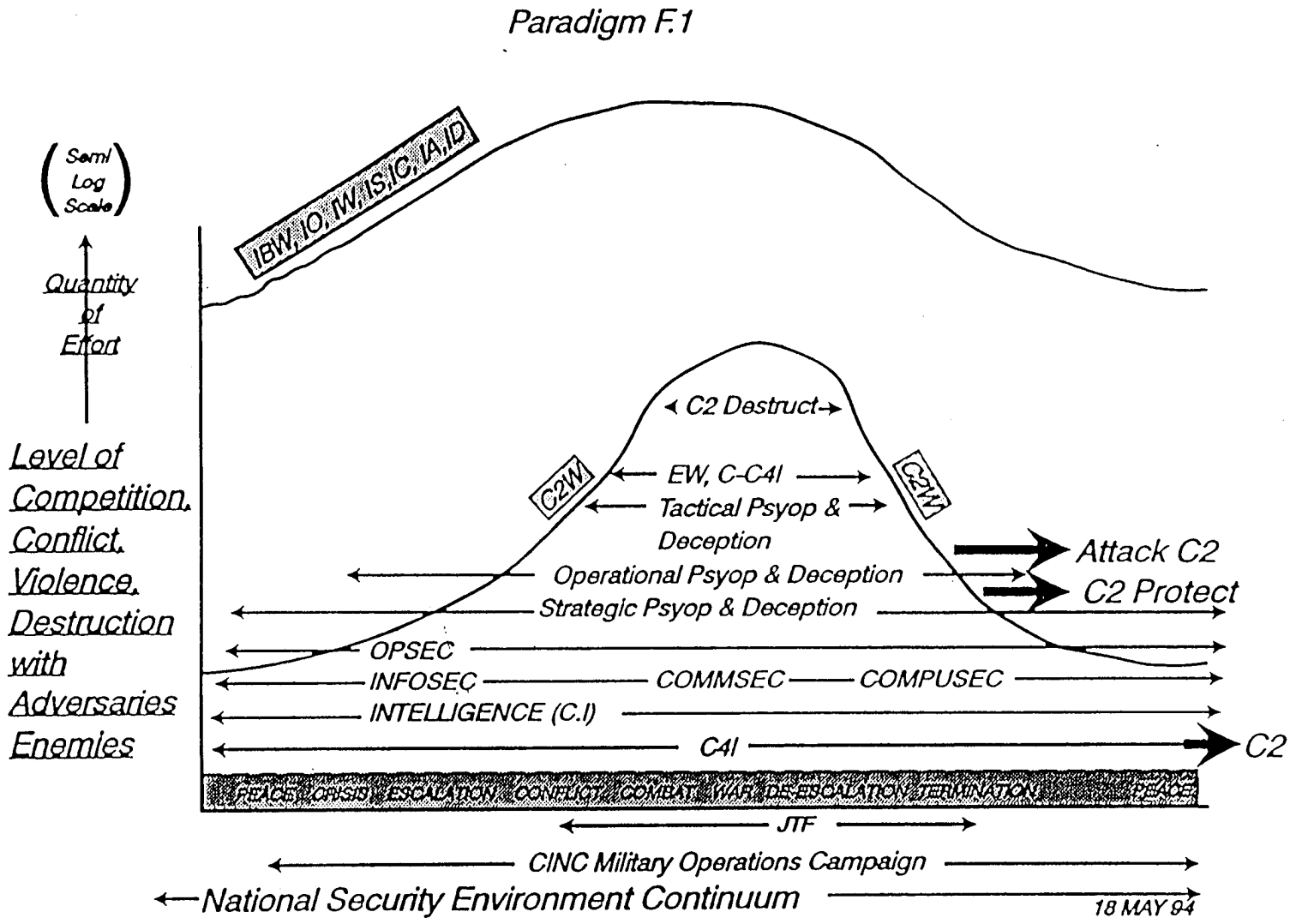

Figure 3. Paradigm F.1 (1 of 3).[From Ref. 28]

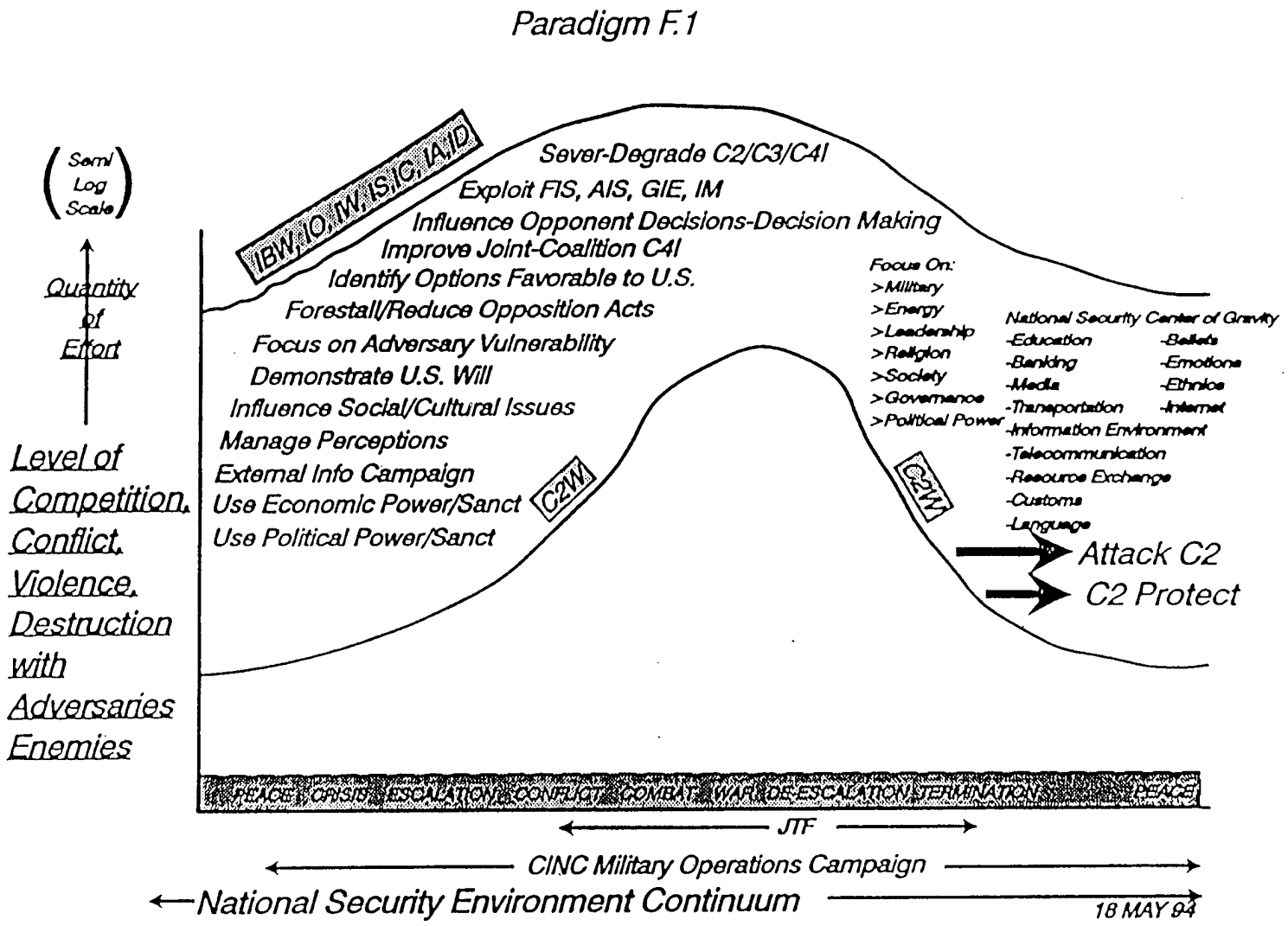

Figure 4. Paradigm F.1 (2 of 3).[From Ref. 28]

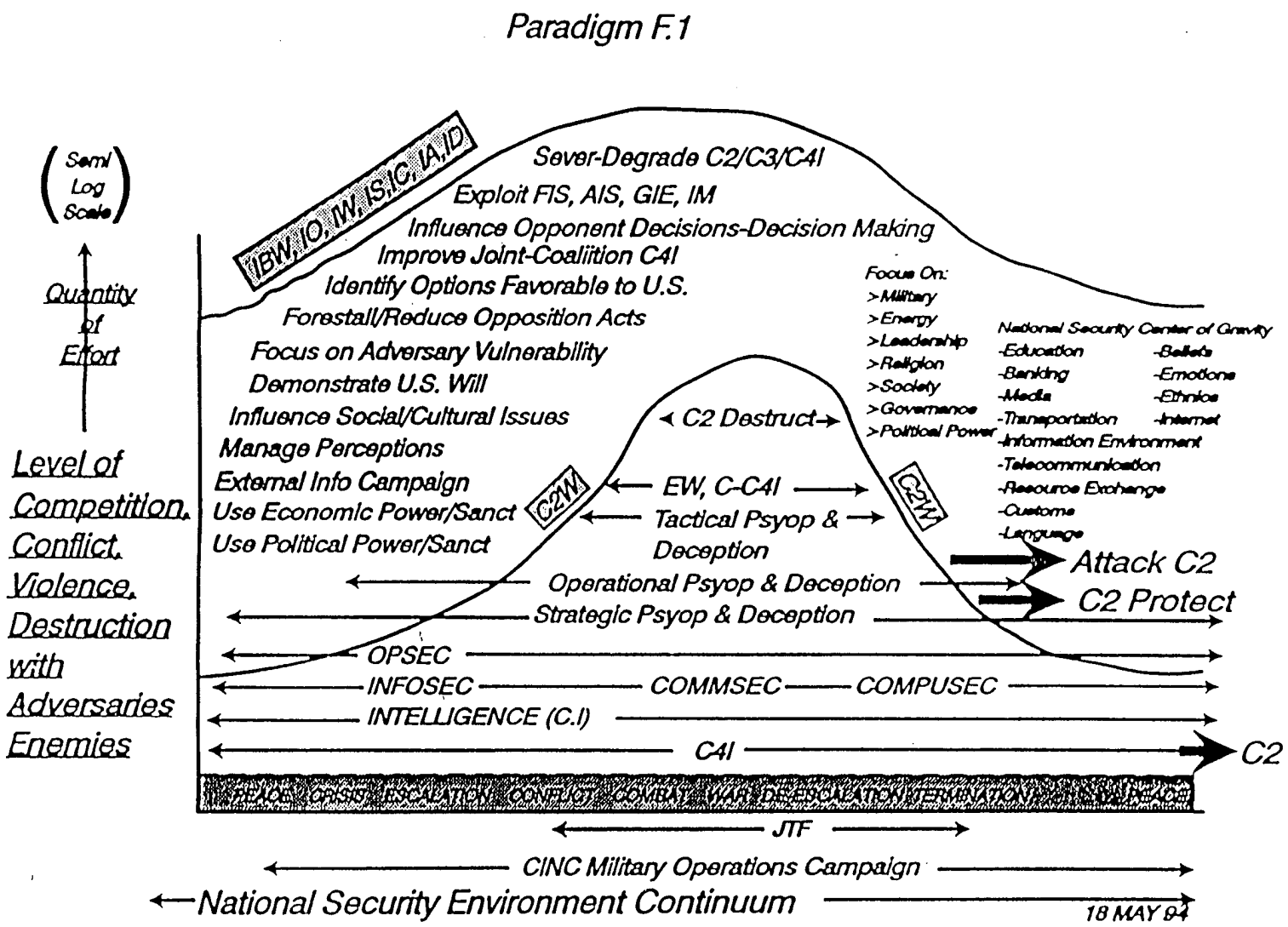

Figure 5. Paradigm F.1 (3 of 3).[From Ref. 28]

Paradigm F (which includes Paradigm F.1 for the purposes of this discussion) is a clarifying tool. In basically two (but expanded to five for ease of explanation) diagrams, one can simply and effectively explain what Information Warfare is. The whole range of sub-components, from military to politics is addressed. The whole spectrum of conflict is viewed. Some specific uses of both Information Warfare and its child, C2W, are stated. Even the place of Information Warfare in everything that comprises the United States is seen. Paradigm F is a powerful way to clearly and concisely explain to virtually anyone what the definition of Information Warfare is.

D. THE BOTTOM LINE

This chapter has been a brief overview of some of the many perspectives of Information Warfare. Some might argue that these points have been anything but brief, but if one truly understands Paradigm F, then one can truly appreciate the enormousness of this "beast" and see that this chapter has only touched the surface. While many different definitions exist for Information Warfare (as well as many different words for Information Warfare), no one definition can fully capture the entire view. If one accepts that a common definition is necessary to facilitate the execution of IW, then one can see the need to be as close to all-encompassing as possible. However, such a definition would need to avoid some of the common pitfalls outlined earlier as well as remember certain key features. Perhaps the most efficient way to accomplish all of these objectives is by using powerful pictures, such as presented by Paradigm F.

III. INFORMATION WARFARE ORGANIZATIONS

A. INFORMATION WARFARE PLAYERS

After settling on Paradigm F as a definition for Information Warfare, the next logical step is to further clarify the entities that exist in the Information Warfare Domain. As described in the previous chapter, the Information Warfare Domain extends to all corners and at all levels of everything that is the United States. This fact would imply that almost everyone is a player on the field of Information Warfare. In reality, not everyone is (but almost everyone). However, more and more people and organizations are embracing the Third Wave as reality and developing Information Warfare strategies as a result. One could argue that there is not much utility in defining an organizational structure where almost anyone and everyone is a player. On the contrary, with such a crowded field, the need is even greater for clarification.

Table 3 on the following page shows a possible breakdown of these players. The leftmost column shows four major categories. The middle column breaks down each of these into smaller subcategories. The final column shows examples of specific organizations or groups of organizations that have a vested interest in Information Warfare. The paragraphs below expound on some of these categories, subcategories, and examples. A detailed discussion of each element in the table is not necessary in the context of this thesis. As a result, some areas will get heavy emphasis (*e.g.*, Department of Defense) while others will only be briefly reviewed (*e.g.*, State and Local Governments). One should note that the Federal Government and National are two separate entries in the table. This is done because the Federal Government is the major player within the National domain and deserves its own category.

MAJOR CATEGORY	SUBCATEGORY	EXAMPLES
International	*e.g.*, Canada	*e.g.*, Dept. of National Defence
National	Public	Academia
		Public Interest Groups
		Media
	Private	Industries
		Associations/Alliances
		Subversive Elements
Federal Government	Executive Branch	Dept. Of Defense
		Other Departments
		Interagency Groups
		Advisory Committees
	Independent Establishments	*e.g.*, CIA, FCC, FEMA, etc.
	Legislative/Judicial	*e.g.*, Senate, House of Representatives, etc.
State & Local Governments	*e.g.*, Texas	*e.g.*, Dept. Of Transportation

Table 3. Information Warfare Players. [After Ref. 29]

One obvious missing piece from this table is the individual citizen. Although the average person definitely has a high interest in IW (*e.g.*, it is the individual's money that will be stolen when a hacker breaks into a bank's computers), this thesis is primarily concerned with organizations and collective entities. Although the role of the citizen is recognized, a detailed analysis of that role is neither relevant nor feasible in the context of this thesis, and thus is only mentioned briefly.

1. International Level

As alluded to in the previous chapter, Information Warfare is not limited to the United States. Although the U.S. has most of the technology and knowledge that is conducive to Information Warfare, many other countries and international organizations are involved. Some are interested in purely the defensive side of IW, some are interested in an offensive aspect against the U.S. (as well as other countries), and some are interested in both. Not much specific information is easily available concerning these endeavors. However, some common trends in the world can be collated to form a generic picture of a viable IW player. This portrait can then be used to create strategies that are defensive or offensive in nature. The latter facet is the crux of this thesis.

2. National Level

As outlined in Paradigm F, the United States is a major player in the Information Warfare game. Almost all corners of society are impacted, from the public to the private. Each area is involved to varying degrees. Note that this definition of National Level excludes the federal government (which is a category of its own in Table 3).

a. Public

The three major players in the Public subcategory are Academia, Public Interest Groups (PIGs), and the Media. As seen in the previous chapter, the academic community has been heavily involved with defining the problem. The media has an obvious role as one of the prime distributors of information at large. As with almost any democratic society, PIGs also are interested in Information Warfare; however, their role is not vital to this study and will thus be ignored.

(1) Academia. While contributing to the debate of IW definitions and terminology, the academic community is also promoting education in the field. Almost every one of the academics listed in Chapter II have at least one major publication to their name. Some are employed on faculties and some are writers for various periodicals (or both). Several civilian schools and universities (*e.g.,* George Mason University) have created courses or concentrations of study related to Information Warfare. More and more public and private corporations, organizations, and bureaucracies are including IW material in their education and training programs.

The Department of Defense has established formal courses of study at all levels of formal education and everyday training. Although the efforts are diverse across the board, more emphasis on standardization (brought about in part by increased dissemination of knowledge) is the current trend. As an example, the National Defense University has created an entire school (the School of Information Warfare and Strategy) dedicated to the study of this discipline. Another example is the Naval Postgraduate School which has restructured an entire curriculum and focused it on Information Warfare. The increasing importance of IW will lead to even more formal programs being established.

(2) Media. The role of the media, as a prime provider of information, cannot be ignored. As one example, Chuck De Caro, former Cable News Network (CNN) correspondent and current president of Aerobureau Corporation[5], preaches what he call "Soft War". Since television has proliferated itself to almost all parts of the world ("global

[5] Aerobureau Corporation is the company that developed the fully integrated airborne journalistic platform. It contains everything a team of journalists needs to do their job, and it is highly versatile (*e.g.*, it can land on almost the smallest of runways).

television"), the media can be used as a weapon. By effective manipulation of "B-Rolls" (video clips), a country's perception of reality can be skewed.[Ref. 30] These ideas will be revisited in later chapters. Thus, the media is definitely involved in IW, willingly or not.

b. Private

(1) Industry. Industry and the business world are also Information Warfare players. The most obvious role is a defensive one in which a corporation desires to safeguard its electronically stored information. As more and more business is being conducted over electronic media, the need is growing to protect that information from manipulation or destruction. As a result, many companies have created information security organizations. Some of the companies with formal IW-related groups include: American Bankers Association, AT&T, Citibank Corporation, Intel Corporation, Motorola, Inc., Silicon Graphics, Inc., and Sony.[Ref. 29] Note that this list is not all-inclusive, but rather provides a sampling of the variety of corporations that are involved in IW.

(2) Subversive Elements. One obvious group of people that cannot be ignored on the IW playing field are the subversive elements. They range anywhere from the teenage amateur hacker and the disgruntled employee to the sophisticated newsgroup clique and the highly organized terrorist cell. These people or groups of people can cause serious damage from an IW viewpoint and must be considered as part of the total IW picture.

The traditional view of a hacker[6] has changed from the *Wargames* paradigm of a lone, exploring kid to the much more dangerous professional. These latter

---

[6] A hacker can be defined as "a computer user who attempts to gain unauthorized access to proprietary computer systems".[Ref. 31]

individuals and groups have turned a typically solo venture into a small (but growing) business enterprise. Today, hackers are not driven by such things as revenge, as they were in the past, but rather by things such as possible financial or political gain. That changing mentality, coupled with the availability of hacker knowledge (*e.g.*, easily accessible newsgroups such as alt.2600 provide tips for hackers as well as programming code segments), has led to a far more dangerous threat than the individual bent on proving a point.

As more and more government and commercial computer systems are being penetrated and exploited by subversive elements, changes are ongoing to counter these endeavors. Thus, one can easily see that these subversive elements are a vital piece of the IW puzzle.

3. Federal Government

Naturally, the U.S. government is interested in Information Warfare. Paradigm F shows the range of government interests. Chapter II offered IW definitions mostly from government sources. Yet, the government has not settled on a consolidated view or strategy for Information Warfare. Instead, each group within the government has its own IW organizations with very little cooperation and sharing amongst the factions (although some improvements in this area have begun).

a. Executive Branch

The highest levels of government have embraced Third Wave principles and taken steps in developing Third Wave thinking and products. As an example, Vice President Al Gore is implementing the concept of a totally networked United States built upon the National Information Infrastructure (NII). The NII is discussed in the next chapter. A large number of

organizations within the Executive Branch of the government have formal groups dedicated at least in part to the Information Warfare mission. A sampling is shown in Table 4 below.

CATEGORY	SUBCATEGORY	EXAMPLES
Advisory & Policy Groups	National Security Council (NSC)	Nat'l Information Infrastructure Task Force
	National Economic Council	N/A
	Nat'l Sec. Telecomm. Advisory Committee	N/A
	Office of Science and Technology Policy	N/A
Departments	Commerce	Nat'l Institute of Standards and Technology
	Defense	USA, USN, NSA, DISA, etc.
	Energy	Sandia Labs, etc.
	Justice	FBI, Computer Crime Unit
	State	Bureau of Diplomatic Sec.
	Transportation	Coast Guard
	Treasury	IRS, Secret Service

Table 4. Executive Branch Information Warfare Players.[After Ref. 29]

b. Department of Defense

The Department of Defense (DOD), charged with protecting the United States from foreign hostile threats, has a large (and sometimes controversial) role to play in Information Warfare. In fact, the majority of organizations within DOD have at least a minor role to play in IW. Some of the major players include: the Office of the Secretary, the Armed Services (Joint

Chiefs of Staff, Army, Navy/Marine Corps, and Air Force), and other groups (NSA, DISA, DIA, etc.). The following paragraphs provide some details about some of these specific entities. The scope of this thesis precludes a detailed discussion of each organization or even a brief discussion of all organizations. As a result, only some of the major actors are included.

(1) Office of the Secretary. The major players in the Office of the Secretary of Defense are: the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASD C3I), the Information Warfare Executive Board (IWEB), the Office of Net Assessment (OSD NA), and the Infrastructure Policy Directorate in the Office of the Under Secretary of Defense for Policy (USDP IPD). The ASD C3I is the principal advisor to the Secretary of Defense (SECDEF) for Information Warfare issues. He is charged with overall direction of IW issues within DOD. The IWEB is chaired by the Deputy Secretary of Defense (DEPSECDEF) and its membership includes: the ASD C3I, the USDP, the Vice Chairman of the Joint Chiefs of Staff (VCJCS), the Deputy Director of Central Intelligence (DDCI), the directors of the National Security Agency (NSA) and the Defense Information Systems Agency (DISA), the DOD Comptroller, a representative from the NSC, and the DOD General Counsel. This interagency and interservice committee manages IW policy, planning, and legal concerns. OSD NA performs IW analysis for SECDEF. The USDP IPD deals mainly with the creation, protection, and maintenance of the national infrastructure (Defensive IW). Of course, each of the organizations discussed in this paragraph have their own supporting staffs that coordinate with other organizations, both inside and outside of DOD.[Ref. 29]

(2) Joint Chiefs of Staff. The Joint Chiefs of Staff (JCS) are responsible for coordinating all military Information Warfare endeavors. There are two major subdivisions

within the JCS: J6K and J38. J6K is the Information Warfare Division and deals with Defensive IW. J38 is the Information Warfare/ Special Technical Operations Division (IW STOD) and works in the Offensive IW realm. A third arm of JCS IW efforts could be the education and training provided by the National Defense University (NDU). [Ref. 29] The specifics of NDU's efforts have been discussed in the section on academia.

Also closely tied to the JCS is the role of the CINCs, who are heavily involved in IW. CINC in this context focuses primarily on the regional CINCs; supporting CINCs, such as Space Command (SPACECOM) and Transportation Command (TRANSCOM), are also involved. CINCs serve as the chief warfighters for a given geographical area. In this capacity, they must be familiar with all aspects of warfare, and thus all facets of IW, from the strategic (CINCs work directly for SECDEF) to the operational (CINC's primary mission) to the tactical (CINC subordinate commanders). While each CINC's organizational structure is slightly different, each has at least a C2W organization and, increasingly, an IW cell.

(3) Department of the Army. As mentioned in the previous chapter, the Army views Information Warfare as a subset of Information Operations. IW is implemented by the military in the form of C2W. As a result, the majority of the Army's efforts are C2W-based. There are basically three echelons of IW endeavors: Army Staff, major command level, and other elements.[Ref. 29] Table 5 shows a summary of the different organizations by echelon. No details of specific activities will be discussed in this chapter. In subsequent chapters, references to some of these organizations will be made. The reader should note the C2W emphasis (supported by intelligence) throughout the Army's organizational structure (*e.g.*, PSYCOM). The Army's entire IO concept is centered around the concept of a "digitized"

battlefield in which information is passed through all hierarchies, even down to the individual soldier.[Ref. 15] Thus, IW is vital to the Army's future.

ECHELON	ORGANIZATION
Army Staff	Ass't Secretary of the Army (Research/Development/Acquisition) (SARDA)
	Office of the Deputy Chief of Staff for Operations (ODCSOPS)
	Office of the Deputy Chief of Staff for Intelligence (ODCSINT)
	Office of the Director of Information Systems for C4 (ODISC4)
Major Command	Intelligence and Security Command (INSCOM)
	Information Systems Command (ISC)
	Training and Doctrine Command (TRADOC)
Other Elements	Land Information Warfare Activity (LIWA)
	Psychological Operations Command (PSYCOM)
	Special Operations Command (SOCCOM)

Table 5. Army Information Warfare Players.[After Ref. 29]

(4) Department of the Navy. The Navy's view of Information Warfare was seen in the second chapter: Exploit, Protect, and Attack. To support that definition, the Navy is trying to focus on the implementation of IW at the operational (*i.e.,* Joint Force Commander or JFC) level. However, there still exists the need for an administrative support arm for doctrine and policy.[Ref. 32] A summary of the Navy's organizations is provided in Table 6.

On the administrative side, the Navy's cryptologic organization (Naval Security Group or NAVSECGRU) has been designated as Executive Agent for Navy IW.[Ref. 33] This means that NAVSECGRU is tasked with coordination of all Navy IW activities. Of course, the Navy Staff is also involved. Specifically, N3/5 (Plans, Policy, and Operations) and N64 (IW Division) along with Naval Doctrine Command (NDC) develop requirements and

systems as well as policy and doctrine.[Ref. 32] In addition, CNET (Chief, Naval Education and Training) is implementing formal IW instruction and training at all layers, from entry-level training (boot camp, officer training, etc.) to senior officer education (*e.g.*, Prospective Commanding Officer's School). [Ref. 29] However, some education programs, such as the Naval War College, the Naval Postgraduate School, and the Naval Academy, fall under the auspices of the Vice Chief of Naval Operations (VCNO) vice CNET.

The operational perspective of Navy IW centers around the recently-formed Fleet Information Warfare Center (FIWC). FIWC is located in Norfolk, Virginia, with a detachment in San Diego, California. FIWC's primary mission is to assist the Fleet CINCs in the creation and implementation of IW/C2W (recall the Navy's definition of IW from Chapter II) "tactics, procedures, and training".[Ref. 32] Supporting these endeavors is the Naval Information Warfare Activity (NIWA) which provides technical support, including research and development, for IW. Of course, Naval Intelligence (N2) supports all Navy IW and C2W efforts.

LEVEL	ORGANIZATION	PRIMARY IW MISSION
Administrative	NAVSECGRU	Executive Agent
	N3/5	Plans & Policy
	N64	Requirements & Programs
	NDC	Doctrine
	CNET	Education & Training
Operational	FIWC	Assist Fleet CINCs in IW/C2W execution
	NIWA	Develop IW technologies
	N2	Provide intelligence support for IW/C2W

Table 6. Navy Information Warfare Players.[After Refs. 29, 32, and 33]

The Marine Corps also has an interest in Information Warfare, albeit focused mainly on C2W. The two major Marine Corps organizations involved are the National Plans Branch (NPB) in the Plans, Policy, and Operations Branch at Headquarters, Marine Corps (HQMC), and the Assistant Chief of Staff for C4I. The former is concerned mostly with IW as it relates to national and DOD policy while the latter is concerned more with traditional C2W missions (*e.g.*, EW, OPSEC, etc.). Also, the Marine Corps has created a working group to coordinate efforts with the other services as well as national organizations.[Ref. 29]

(5) Department of the Air Force. Chapter II outlined the Air Force's definition of Information Warfare which can be summarized as enhanced C2W with some added value. Towards that end, the Air Force has created an extensive Information Warfare organizational structure. This structure can be broken down into four major components: Direction and Administration, Procurement, Support, and Execution. A summary table, Table 7, is provided at the end of the paragraphs discussing each of the four components.

At the top level in the Air Force, the Chief of Staff has directed that the Assistant Chief of Staff for Intelligence (ASCI) and the Deputy Chief of Staff for Operations (XO) coordinate implementation of IW in the Air Force. ASCI is writing the policy and doctrine with monitoring and consent by XO as well as by the Assistant Chief of Staff for C4 (SC). In turn, the Doctrine branch (XOX) publishes the doctrine.[Ref. 29] These organizations form the Direction and Administration component.

Procurement of IW systems is also important, so the Assistant Secretary of the Air Force for Acquisition (ASAF/AQ) and Air Force Materiel Command (AFMC) are involved. Two primary subsidiary organizations involved are Rome Laboratory and the

Electronic Systems Center (ESC)[Ref. 29] Rome Lab deals with research of IW systems while ESC is focsued on acquisition of IW systems. These groups collectively form the second component.

Any kind of IW or C2W operation needs to be supported by intelligence and thus the ACSI is involved from that aspect as well via the Air Intelligence Agency (AIA) and its subordinate specialty organization, the Air Force Information Warfare Center (AFIWC).[Ref. 29] One of the more critical nodes in this organizational network is AFIWC. AFIWC "supports operations, campaign planning, acquisition and testing."[Ref. 34] To this end, AFIWC provides Information Warfare Support Teams (IWSTs) which are dedicated to supporting the warfighter.[Ref. 34] ASCI, AIA, AFIWC, and IWSTs comprise the third component.

The fourth and final component is execution. For that purpose, the Air Force has recently stood up the first squadron dedicated entirely to Information Warfare: the 609th. The actual composition of materiel and personnel for this squadron as well its specific missions are all still very fluid.[Ref. 35] An expanded role for XO and SC are anticipated in the future in the Execution component.[Ref. 29]

PRIMARY MISSION COMPONENTS	ORGANIZATIONS INVOLVED
Direction & Administration	XO, ASCI, XOX, SC
Procurement	ASAF/AQ, AFMC, Rome Lab, ESC
Support	ASCI, AIA, AFIWC, IWSTs
Execution	609th IW Squadron, XO, SC

Table 7. Air Force Information Warfare Players.[After Refs. 29, 34 and 35]

(6) Other Organizations. Three other DOD organizations are also worth mentioning for their role in DOD Information Warfare: NSA, DISA, and DIA. Numerous other

supporting organizations also contribute somewhat to the Information Warfare mission, but they are too numerous to list here.

The Defense Intelligence Agency (DIA) is involved in IW for the necessary intelligence support aspect and coordinating the efforts of the individual services.[Ref. 36] The specifics of the service intelligence organizations were seen earlier under their respective departments.

The Defense Information Systems Agency (DISA) is the central control point for Defensive Information Warfare (DIW) endeavors within DOD. DISA is tasked with defending the Defense Information Infrastructure (DII), the DOD's component of the NII.[Ref. 37] The major IW players at DISA are: the Directorate of Operations (D3), the Information Warfare Division (D34), the Center for Information Systems Security (CISS), and the Automated Systems Security and Incident Support Team (ASSIST).[Ref. 29]

As the traditional providers of Signals Intelligence (SIGINT) (*e.g.*, EW), the National Security Agency (NSA) is also heavily involved in Information Warfare. The Information Warfare Director is a senior level military officer or civilian who works directly for the Director of NSA. He is charged with representing NSA's interests and coordinating with other agencies and entities. The Information Warfare Support Center is found in G Group. Other NSA players include: K Group, V Group and X Group.[Ref. 29]

Overall, the Department of Defense is the largest single participant of the federal government in the Information Warfare realm. As prime providers of national security, DOD plays on both the offensive and defensive side of Information Warfare. The numerous

organizations involved in many different facets of IW require a significant coordination effort from the highest levels within the department as well as from the individual organizations.

c. Legislative/Judicial

Not only is the Executive Branch involved with Information Warfare, but the other two branches of the federal government are involved as well. The Judicial Branch is obviously involved to enforce statutes and resolve legal and constitutional issues. As the etherealness of the Information Warfare domain is placed under legal scrutiny, the Judicial Branch will be required to rule on enforcement of IW laws. The legal considerations of IW will be expounded upon in a subsequent chapter.

The Legislative Branch has an important role to play in the creation of laws regarding Information Warfare. Numerous committees and subcommittees in both the Senate and House of Representatives have a role. In the Senate the following committees or subcommittees are involved in some fashion: Appropriations, Communications, Armed Services, Intelligence, Regulation & Government Information, and Terrorism, Technology and Government Information. In the House, the following are significant: Appropriations, Budget, Telecommunications and Finance, Government Management: Information and Technology, Crime, Intelligence, National Security, and Technology.[Ref. 29]

d. Independent Establishments and Government Corporations

The last component of the federal government that needs to be addressed are the various independent establishments and government corporations. Three obvious examples are worth mentioning: the Central Intelligence Agency (CIA), the Federal Comminations Commission (FCC), and the Federal Emergency Management Agency (FEMA). CIA is the

prime provider of intelligence at the national level so is an obvious player. The FCC regulates communications within the United States, both foreign and domestic. DISA works closely with the FCC in protecting the DII. FEMA is involved with IW from the national disaster perspective, including national security emergencies and terrorist incidents.[Ref. 29]

4. State and Local Governments

The role of state and local governments in Information Warfare needs only to be mentioned in passing. More and more states have enacted statutes for computer crime and other IW issues. Although this role is not critical to this thesis, it is something to bear in mind.

B. THE INFORMATION WARFARE FIELD

The Information Warfare playing field is crowded. A large number of organizations have stated IW objectives. This chapter has attempted to give the reader a brief overview of the multitude of players involved as well as an introduction to the complexity of their respective organizations. By no means are these descriptions meant to be all-inclusive. Rather, they are designed to give the reader a feel for the quantity and disparity of organizations involved in Information Warfare.

The opening paragraph of this chapter stated that under the Paradigm F structure, anyone and everyone was a player on the Information Warfare field. While this may be very true to some extent (especially in light of the myriad of organizations mentioned in this chapter), there is little benefit in such a statement. In fact, a detailed discussion of the many players (and not just a blanket statement), appropriately partioned, is necessary to better understand the Information Warfare domain.

Of course, the inclusion of everyone on the playing field (albeit hypothetically somewhat segregated by organization) has its drawbacks. The potential exists for duplication of efforts or even omission of a function (under the presumption that another organization is charged with that mission). Also, having a crowded playing field potentially increases the vulnerability of friendly forces (the enemy could easily hide in the midst of so many friendly forces). This could even lead to Information Warfare fratricide (friendly forces may unintentionally destroy or damage a friendly asset while attempting to oust an enemy).

Thus the central problem becomes one of coordination. In order to be fully effective, a central focus is needed. Although the many and varied organizations are being guided somewhat by a common vision, there is no clear-cut dissemination of roles and responsibilities from the highest levels. This problem of a uniform and focused effort is not unique to the organization problem. In fact, it was seen in the previous chapter on definitions. A discussion of the "optimal" organizational configuration is reserved for Chapter VIII.

In summary, there are a large number of varied entities that each have their own objectives and definitions on the Information Warfare playing field, and all are moving loosely in the same direction. With such a force on the IW field, the discussion should next logically turn to the technologies that these players could, should, or would use to perform their missions.

IV. INFORMATION WARFARE AND TECHNOLOGY

A. TECHNOLOGICAL REVOLUTION

The Third Wave revolution has been brought about in large part due to the explosion in technological advances. Technology has become cheaper and more powerful. Bandwidth for communications is increasing. Computer processor power is doubling every 24 months. Computer memory is tripling every 18 months. Computer storage media are doubling in capacity every 24 months while the cost is halved every 18 months.[Ref. 34] Computers are becoming more commonplace and are increasingly tied together via networks. The Internet is growing exponentially. Satellites are becoming smaller and more powerful. Advances in voice, data, and video distribution are leading to more effective communications. Today's breakthrough developments become obsolescent tomorrow. More and more organizations, government and commercial, are embracing these advances with open arms.

Such is the dynamic environment for today's world. This technological explosion has thrown the role of Information Warfare to the forefront. Technology has facilitated the growth of IW into an increasingly solid warfare discipline. However, while enabling IW to be performed, technology has also increased vulnerabilities, which, in turn, leads to more IW. This chapter will explore some of the advances that have brought about this change. Since the technological growth is moving so fast, it is impossible to detail every new development here. In fact, some or perhaps all of the technologies discussed herein will soon be replaced with faster, more efficient ones.

The goal is to provide the reader with a feel for the types of technologies that can promote or degrade Information Warfare. Some specific technologies will be briefly overviewed.[7] The role of these technologies in Information Warfare will also be briefly addressed along the way. Subsequent chapters will expound on some of the technologies discussed in this chapter.

B. ENABLING TECHNOLOGIES

Some might ask if technology has a defined role in an Information Warfare application, specifically from a military perspective. The answer, of course, is yes. The Army is developing the "21st Century Soldier" concept.[Ref. 38] This warrior will be armed not only with a weapon, but also with a computer and full range of sensors. Information will be relayed in full duplex in near-real time.

Another specific IW example can be seen in the Psychological Operations (PSYOPS) realm.[8] The "Commando Solo" aircraft is specially designed for PSYOPS. It is full of communications equipment and computers. The aircraft is flown over enemy locations (and can even be used against a civilian populace). It plays music or biased news broadcasts or even special messages. The idea is to break down the enemy's will to fight. In fact, this was used both in Operation Desert Storm and Operation Support Democracy.[Ref. 39] This platform is a fine example of the military and technology working together to create a formidable Information Warfare weapon.

---

[7] Throughout this chapter, specific companies or their products will be mentioned. By no means do such references imply an endorsement for these goods or services.

[8] Recall that PSYOPS are a subset of C2W which in turn is a subset of IW.

These enabling technologies can be broken down into four major categories (which themselves can be further decomposed): Computers and Networks, Telecommunications, Other Pertinent Technologies, and Emerging Technologies. Each of these categories is discussed in further detail in this chapter. Some specific examples of each category are included. By no means should these examples be viewed as all-inclusive. Instead, they should be seen as an example of the role that technology plays in Information Warfare. Table 8 is presented at the end of this section to provide a summary of the technologies discussed.

1. Computers and Networks

The most obvious enabling technology for Information Warfare is the computer. Computers are becoming more visible in almost every facet of society all over the world. Technology is allowing for more uses of powerful computers. When one thinks of an "Information Warrior," the immediate impression is of someone sitting behind a computer terminal. This is an apt analogy (but not the only one); the computer is one of the most powerful weapons, both offensive and defensive, that can be used in Information Warfare.

a. Computer Advances

As mentioned in the opening paragraph of this chapter, computers are evolving at dramatic rates. Processors, storage, and memory are all becoming more powerful and cheaper. This leads to more possibilities for computer use (*e.g.*, desktop video teleconferencing). Computers are also becoming more portable (discussed later in this chapter), which facilitates any IW application (*e.g.*, portable computers are less vulnerable to physical attack). Palmtop computers have emerged that permit networking and high processing power in a machine that can be carried in a pocket.

One example of a specific robust computer technology is parallel computing. Parallel computers execute numerous machine instructions simultaneously (as opposed to sequentially in traditional computers). This allows for faster processing of more information. For today's world of massive information flows, this type of computer is a definite asset. From an IW perspective, parallel computer architectures offer some protection against "chipping"[9]; if one processor fails, another could continue the work, albeit at a degraded capability. Along the same lines, multiple parallel processors are easier to protect because of their redundancy (if designed correctly, the failure of one does not preclude continued operation). Finally, once inside an enemy's computer system, our own parallel computers offer the ability to retrieve and process large amounts of information.[Ref. 40]

b. Networks

A computer is only a fancy typewriter or calculator if it is not connected to other computers. Networked computers are an essential part of today's world and thus an essential part of the IW domain. Computers can be linked together in an infinite number of ways, from Local Area Networks (LANs) to Wide Area Networks (WANs). A LAN could merely connect several computers in one building or be tapped into other LANs to form a larger network.

Networked computers allow for more efficient operations. Data can be shared between users. Communications can be vastly improved (*e.g.*, via use of electronic mail). Users can query other computers and users through such things as the Internet (discussed in more detail later). More powerful software packages installed on increasingly powerful hardware platforms facilitate networking. A perfect example is the 1996 release of Lotus Notes Suite. This product

[9] Chipping is an Offensive IW technique that is discussed in the next chapter.

allows for traditional functions (word processing, spreadsheets, graphics presentations, etc.) as well as the interactive sharing of that information amongst users. Also included are such things as electronic mail capabilities, interactive database queries, and Internet access.[Ref. 41]

While promoting efficiency, this type of networking also enhances Information Warfare. Almost any computer security expert will say that the best way to protect a computer is to cut off its ability to communicate with other computers. While this is a very true statement, it is not feasible in today's world. As organizations become smaller with an increased workload, they must become more efficient, and networks facilitate this. Networks demand effective network security (discussed later in this chapter) to safeguard information (Defensive Information Warfare). At the same time, networks allow for penetration and exploitation by adversaries (Offensive Information Warfare).

c. Internet

The "network of networks" is the Internet. The Internet is a semi-tangible, although highly ethereal, worldwide network of computers. It crosses all barriers of language and culture. Through powerful navigation tools such as Netscape, users can garner a wealth of information about a variety of subjects. It is also extremely easy to use via robust "search engines". These tools allow for the collection of large amounts of data in a relatively short time.

The Internet is definitely an IW weapon. It allows for the collection of large amounts of open source intelligence which can then be used to launch IW attacks. In fact, the Internet is so useful that many organizations need access to it to accomplish routine functions. These entry points can serve as gateways for penetration and exploitation. On the flip side, these same gateways create headaches for systems security personnel who must protect them.

The Internet is also experiencing a major paradigm shift of its own. Traditionally, information from the Internet had to be collected with a software program that could interpret that information or convert it to a usable format later. If no such software tools were available, the user had to get one or do without the information. Now, however, there is a shift to a dynamic and virtual Internet whereby needed software tools could be made available upon request. For example, a user requests data in a particular format. The server responding to the request queries the user's system to determine availability of the required software. If it is not available, the server retrieves a temporary copy of that program from its own database or another server and opens it for the user. Sun's Java programming language (via use of "applets") is an example of the first steps in this emerging technology.[Ref. 42] While strengthening data collection and analysis capabilities, this technology also presents new avenues for attack as well as increased security concerns.

d. Architectures

Networked computers have led to the creation of information architectures at various levels: the Global Information Infrastructure (GII), the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII). The GII is currently only a vision in the worldwide community. The latter two are specific to the United States and were mentioned in the previous chapter.

The GII is a concept of a totally interconnected world. At the international level, governments would be passing back and forth anything from marketing information to scientific data. The goal is to promote world stability and prosperity by the exchange of information and technology.[Ref. 43] The GII also includes initiatives to involve poorer nations in the process.

Such countries currently do not have the supporting technology base to participate in the GII. However, the GII would help create these needed infrastructures by leapfrogging technology (*i.e*, bypassing the installation of traditional infrastructures and moving straight to more modern ones.[Ref. 44]

The NII is a more tangible version of the GII within the United States. It is an initiative to unite federal, state, and local governments with the business and industry worlds. The main goal is to promote sharing of information and resources as well as to conduct business electronically. There is a national level task force (involving all of the major players) that is overseeing the creation of the NII.[Ref. 45]

The DII is the Department of Defense's version of the NII. It is being run by DISA. The goal of the DII is to provide a common architecture across DOD for communications, information exchange and processing during all levels of conflict, from peace to war.[Ref. 37]

These overarching information architectures are also players in the IW arena. The obvious needs for security in such large networks are major reasons for the growth of the Defensive Information Warfare (DIW) industry and discipline. These kinds of networks also provide a convenient entry point for network penetration to accomplish any number of IW attacks at many different types of systems. The evolution of the GII into reality (if it does so) is a major consideration for this thesis and will be addressed in a later chapter.

2. Telecommunications

One of the principal characteristics of a Third Wave world is a reliance on information. That information must be moved from place to place. Thus enters telecommunications as the

primary medium for the transfer of that information. As information becomes more and more dominant in all aspects of world society, the telecommunications industry will continue to thrive. This prolific use of the electromagnetic spectrum abounds with opportunity for Information Warfare tactics and techniques.

This portion of the chapter examines some of the existing and future telecommunications technologies. Three separate communications groups are examined: traditional communications, satellite communications, and cellular communications. Due to the vast and dynamic nature of this field, not all possible systems are explored. Several emerging technologies in telecommunications are reserved for a separate subsection later in this chapter.

The discussions presented here present only a rudimentary examination of the technologies in question. The real application of these technologies in an Information Warfare environment is extremely complicated. A detailed analysis of the many factors involved (*e.g.*, modulation techniques, error correction schemes, protocols, various transmission losses, compression schemes, etc.) is impossible for a document of this nature. For a further look at the workings of these systems, the reader is referred to the many sources referenced in this chapter as well as several others listed in the Bibliography at the end of this document.

a. Traditional Communications

Traditional communications refer mainly to the use of "old" (*i.e.*, existing) infrastructures. Although there is nothing traditional about the ongoing revolution in this arena, it serves as a convenient grouping category. Included in this category are such things as traditional voice communication *(i.e.*, phone) networks, microwaves, and fiber optics, with an

increasing transition from analog to digital technology. Each of these specific categories has its own input to the world of Information Warfare.

(1) Copper Wire Telephone Communications. Today's telephone is more than an instrument for voice communications. With a modem and a computer attached, a telephone line serves as a gateway to the networked world. Existing telephone systems can pass voice, data, and even video. Current initiatives and emerging systems allow for an even more efficient (*i.e.*, higher throughput) transmission of this information using existing systems (with different modulations techniques) as well as using entirely new systems (ISDN, fiber optics, etc.). This leads to an infrastructure that is increasingly vulnerable to Information Warfare.

A basic understanding of the most common type of telephone communication is necessary before proceeding. A typical phone call requires the conversion of voice data into electronic form that can be transmitted over copper wire to the receiving end, The telephone number dialed sets the path that will be taken by the message. Basically the path goes from the phone to a local loop, through a telephone company switch, through a series of interexchange channels (IXCs), through a switch near the receiving end, and finally into the receiving party's phone where the signal is reconverted into voice format.[Ref. 46] This path is known as a voice grade circuit (VGC). A VGC in the public domain is most often accomplished via the Public Switched Network (PSN), which is typical phone service where equipment is shared by a multitude of users. Another option is using a dedicated line to establish a private connection; this requires an exclusive line not shared by the public.

In the past, the majority of this voice-to-electronic signal conversion had been accomplished via analog techniques. Today, the push is almost entirely digital, using not

only existing copper wire paths, but also new transmission media. The main focus is on increasing the bandwidth (and thus throughput) of transmissions. A VGC can accommodate up to 19.2 kbps (kilobits per second). Other related terms and data rates include: narrowband circuits (56 kbps to 1.5 M(mega)bps), wideband circuits (1.544 (*i.e.*, T1 line) Mbps to 45 Mbps (*i.e.*, T3 line)), and broadband circuits (greater than 45 Mbps).[Ref. 47]

(2) Integrated Services Data Network (ISDN). One example of these new initiatives is the leased service called Integrated Services Data Network (ISDN). The transmission medium for ISDN is either coaxial cable (*e.g.*, like the one used for standard television cable service) or microwave (discussed later). There are two types of ISDN service: basic access and primary access. Basic access is designed primarily for the individual user or small business. It is a digital multiplexing technique that uses two 64 kbps "B" channels for transmission of voice, data, or video (including such things as Internet access) and a 16 kbps "D" channel for signaling and control. The two B channels can also be combined to form a single 128 kbps channel. Primary access is intended for use by larger entities. It consists of multiplexing numerous B channels. There are different standards for the United States (23 B and 1 D channels) and Europe (31 B and 1 D channels).[Ref. 46]

ISDN is fully compatible with Information Warfare. The increased data throughput means faster data collection and analysis capability. New transmission media (*e.g.*, coaxial cable) requires development of new penetration technologies. As ISDN becomes more prolific, more players could become involved (*i.e.*, increased availability and ease of use promotes IW potential). New methods to maintain security is also a concern.

(3) Microwave Communications. Another pertinent technology is microwave transmission. Microwave transmissions involve direct line-of sight transmissions over Super High Frequency (SHF) ranges (1 to 30 Ghz (Gigahertz)) between two points. Microwave technology provides many of the same services as offered by copper wire transmissions (voice, video, or data), but at a much higher throughput (over 100 Mbps in some high-end digital systems [Ref. 48]) using multiple channels. Microwave antennas are generally mounted on towers that are spaced 25 to 30 miles apart.[Ref. 47] Microwave transmissions can be either analog or digital. They can be used for anything from long-distance telephone service to college campus network transmissions to military digital networks.[Ref. 48]

Microwave communications offer great opportunities for Information Warfare. Microwave transmissions have been susceptible to classic Electronic Warfare techniques (*i.e.*, interception, jamming, etc.) since their inception. Increasingly, digital transmissions at high data rates demand a refinement of old methods. As new applications for microwaves are developed (*e.g.*, LANs), new security and penetration issues also emerge.

(4) Fiber Optics Communications. A final example of a new application of traditional telecommunication technology is fiber optics. Fiber optics is a new and more efficient way to perform traditional functions, from phone and data service to LAN connectivity. New applications for fiber optics are also emerging and will be discussed in the section on emerging technologies.

Fiber optics technology involves the transmission of a light wave. Information is converted from its natural state of electric pulses into a series of light pulses. An optical source (such as laser emitting diode (LED)) then transmits these pulses from one terminal

to another through very thin (but shielded) glass strands. Along the way, repeaters (generally spaced no more than 30 miles apart) regenerate the pulses to maintain integrity of the transmission. At the receiving end, the light pulses are then reconverted to electric format for use.[Ref. 47]

Fiber optics offer many advantages over older communications media. It offers virtually infinite bandwidth. Fiber optics components are smaller, lighter, and more flexible than other communications systems. Transmissions are not very vulnerable to electromagnetic interference. Also, fiber optics are relatively secure; transmissions are hard to intercept undetected.[Ref. 48] However, one drawback is that fiber optics, like most traditional communications, are not very portable. Thus, the potential uses of fiber by organizations that depend on mobility (*i.e.*, the military) are limited.

Thus, fiber optics offer large challenges and potential for Information Warriors. Unlimited bandwidth theoretically means unlimited throughput (limited only by the transmission technology). Security administrators on the DIW side can breathe a little easier with a fiber optics system. On the flip side, OIW players are challenged to penetrate fiber optics systems undetected.

b. Satellite Communications

Satellite communications are a mainstay of today's traditional telecommunications environment (as discussed in the previous section). They also offer other applications, from military (*e.g.*, reconnaissance) to commercial (*e.g.*, VSAT--discussed below) to private (*e.g.*, television and telephone service). Each of these applications offers potential use

in another Information Warfare to the extent that satellite communications deserve a section of their own.

The basic ground satellite transmission begins with a user requirement. The information (voice, data, or video) is sent to a ground station via traditional telecommunications media. This information is then transmitted ("uplinked") to an orbiting satellite. This information can be passed to other satellites but eventually is transmitted ("downlinked") to the receiving ground station. Finally the information is sent to the user on the receiving end via traditional methods.[Ref. 46] The actual process is much more detailed due to a large number of variables (*e.g.*, satellite orbit, distances, frequency ranges, etc.), but is presented here in simplified format to ensure a basic understanding of the technique.

Satellite communications offer both advantages and disadvantages. They offer high throughput with low error rates at relatively stable costs. However, satellites are not easily designed or launched and always involve a delay in time (due to the large distances signals must travel). They are also susceptible to interference and interception (although they are becoming increasingly less vulnerable due to such things as new modulation techniques (*e.g.*, Code Division Multiple Access--CDMA)).[Refs. 47 and 48] In any case, satellites are a definite part of the telecommunications world into the foreseeable future.

A large portion of the current initiatives in new satellite technology are Low Earth Orbit (LEO) satellite projects. A LEO satellite orbits very quickly, fairly close to earth (generally below 1000 km [Ref. 49]). Since the area of coverage by LEO satellites is less than higher orbit ones, more satellites are required. Two examples of ongoing LEO projects are Iridium and Teledesic. Iridium is expected to be operational in 1998 and will consist of 66 satellites and six

spares orbiting anywhere from 670 km [Ref. 50] to 780 km [Ref. 51] above the earth. One of the most comprehensive and concise views of Iridium says that Iridium, which will virtually eliminate the need for ground stations, can be best defined as

> a wireless personal communication network designed to permit any type of telephone transmission - voice, data, fax, paging - to reach its destination anywhere on earth, at any time. It will revolutionize worldwide communications in the commercial, rural, and mobile sectors by providing portable universal service.[Ref. 50]

On the other hand, Teledesic, expected to be operational by 2001, is envisioned to have 840 satellites with as many as 84 spares, orbiting at about 700 km.[Ref. 51] While Iridium is focused on cellular communications, Teledesic will target the data communications environment, with such ideas as a wireless Internet.[Ref. 52]

At least three other specific technologies in the satellite realm are worth mentioning. These are the Direct Broadcast Satellite/Global Broadcast Service (DBS/GBS), Very Small Aperture Terminals (VSATs), and International Maritime Satellite (INMARSAT). DBS is a new one-way ("broadcast") technique for disseminating video products (*i.e.*, television) on 200 possible channels at a high rate (23 or 30 Mbps) to individual subscribers with small satellite dishes. The satellite constellation consists of three geostationary satellites orbiting at 35,680 km.[Ref. 53]. GBS is a DOD initiative built on the ideas of DBS. GBS allows one-way transmission of critical information at up to 23 Mbps to deployed warfighters.[Ref. 54] Currently, the military is using existing commercial geostationary satellites for these transmissions. The goal, however, is to have a dedicated military geostationary constellation for GBS. VSAT is a low-cost technique that is currently in use in commercial enterprises around the

world. For example, credit card transactions use VSAT terminals for verification. VSAT communications occur at speeds up to 64 kbps.[Ref. 48]

INMARSAT is an old system (1979) that was originally designed for maritime communications. Today, INMARSAT is used around the world on ships as well as on land and in aircraft. Several different INMARSAT systems exist today. INMARSAT-A is the old maritime standard for voice and low-rate data transmissions. INMARSAT-B is an improved version of INMARSAT-A that uses digital technology and allows faster data transmissions (up to 64 kbps). INMARSAT-M is a portable voice and data system (2400 bps). INMARSAT-C is an even smaller, but slower (600 bps), portable system. Additionally, several types of aircraft systems exist. INMARSAT satellites are geostationary (35,786 km). In the future, improved satellites are scheduled to be launched as well as a whole new system (ICO or INMARSAT-P) that will offer an alternative to cellular communications.[Ref. 55]

Each of the satellite technologies discussed have OIW or DIW potential (or both). Satellite transmissions are vulnerable to classic EW techniques. Broadcast systems allow for transmission of very high data rates. While this may increase the information advantage, such systems are also vulnerable to interception and jamming. The VSAT infrastructure offers potential for clandestine activities. Who is going to question a VSAT terminal ostensibly used for verifying credit card purchases in a third world country? In reality, such terminals could serve as a launch pad for IW attacks against friendly nations by terrorist organizations, for example.

An increasing reliance on LEO systems will clutter the LEO space environment which enhances the IW potential. For example, an OIW team penetrates a satellite control

computer system and changes one or more of the satellite's orbital parameters (most satellites are programmable and steerable). The resulting orbit change could cause a collision with another satellite which causes a catastrophic chain reaction (picture the 900 new satellites conceived in the Iridium and Teledesic projects along with the systems that are already in place). Although this scenario seems a bit drastic and perhaps far-fetched, it is feasible. Other lesser means, could include merely turning the satellites off at a critical time or causing certain components to fail at a predetermined time.

c. Cellular Communications

One of the hottest topics in the telecommunications world today is cellular communications. They began in the 1970s. By 1985, an analog cellular standard, called Advanced Mobile Phone System (AMPS) was in place in the United States. However, the push towards digitization has created several new standards in the U.S. These new standards mark a change from mostly Frequency Division Multiple Access (FDMA)-type schemes to a combination of FDMA and either Time Division Multiple Access (TDMA) or CDMA techniques. The current European standard is known as the Global System For Mobile Communication (GSM) and uses TDMA and FDMA. Other parts of the world have their own cellular standards which are not necessarily compatible with U.S. or European standards (which are currently incompatible with one other).[Ref. 56]

An infinite number of cellular system configurations is possible. The simplest system might consist of one or more radios, cellular antennas (possibly including satellites) and a supporting infrastructure (*e.g.*, telephone switching company). In this basic system, an individual places a call with a cellular phone while driving in a car. The call is routed through the nearest

cellular antenna and is routed to a mobile telephone switching station. The call then enters the traditional telephone switching network (land lines or satellites), where another individual receives the call on a standard wall-mounted phone. As the conversation continues, the driver of the car begins to fade from the cellular antenna's coverage and begins to be picked up by another antenna. The call is then automatically "handed off" to this new cellular antenna. These geographic sectors of control by one or more cellular antennas are called "cells" and are roughly hexagonal in shape. Cellular transmissions are generally low power. Thus, antennas are fairly close together (no more than 40 or 50 miles apart). [Ref. 56]

The future for cellular communications is exciting. One current trend in cellular technology is Personal Communications Services (PCS). PCS is an extension of digital cellular techniques to create wireless networks that are very portable, even down to the individual user for the transmission of voice, data, or video. These PCS networks will be able to directly tap into existing infrastructures such as the public switching stations. Of course, PCS will require the emergence of a very sophisticated supporting infrastructure (the details of which are not fully defined).[Ref. 57] Other future trends include such things as navigation and positional data via cellular phones. Cellular antennas will also evolve to "microcells" which are mounted on lampposts and cover 1000 meters.[Ref. 56] Another trend is the Mobile Internet Protocol (IP) concept which will facilitate access to the Internet via cellular systems.[Ref. 58]

One of the greatest problems presented by the onslaught of cellular technology, and thus one of its greatest contributions in the Information Warfare domain, is security. Numerous concerns exist about the lack of security in today's cellular environment. These problems must be overcome in order for cellular communications to evolve into a secure and

reliable alternative to traditional communications. An efficient cellular security plan must safeguard at least the following information: call setup information (*e.g.*, calling card information for a long distance call), voice and data information, users' locations, users' identification, and users' calling patterns. From an offensive standpoint, any of those vulnerabilities could be exploited or attacked at any number of different areas of the cellular system: transmission towers, switches, cellular or phone company databases, network interconnects, roaming service provider, the cellular phones themselves, etc. At least four different security schemes are in place or emerging in the cellular world: Mobile Identification Number/Electronic Serial Number (MIN/ESN) (an AMPS security system), Shared Secret Key Data (SSD) (for use by PCS systems with CDMA or TDMA), Token Based Security Triplets (for the GSM standard), and Public Key (an emerging technique whose details and applicability have not yet been fully defined). For further information on these systems and a detailed introduction to cellular security, the reader is referred to Chapter 10 of *Wireless And Personal Communications Systems.*[Ref. 56]

3. Other Pertinent Technologies

Several other key technologies cannot be ignored in the Information Warfare domain. Several have been hinted at already but require additional discussion of their own. These include: sensors and space, security, and a "miscellaneous" category (for small but important points that do not conveniently fall into any of the other categories).

a. Senors and Space

Sensors and space will have increasingly important roles in Information Warfare. The current trend in satellite and sensor technology is a decrease in cost and size with a commensurate increase in performance. As the world becomes more networked and conflicts

become more localized, the uses of satellites will become more prolific. These types of satellites must also have a wide variety of very accurate sensors that transmit their data in near-real time and should be able to be launched locally. At the same time, such sensors should be mostly passive and increasingly visual (the mindset of "a picture is worth a thousand words" enters here). Of course, sensor technology need not be solely space-based. The scenario described in Chapter I calls for microsensors with diverse capabilities (infrared, visual, acoustic, etc.). Technology allows for this scenario to evolve into reality.[Ref. 6]

b. Security

Security, the cornerstone of the defensive side of IW, has been discussed at several points in the sections on specific technologies. Yet, at least one additional element needs to be specifically addressed, that of network security. Network security involves everything from encryption to authentication to firewalls. One should bear in mind that a network in this context can be anything from a LAN to a WAN to an individual computer hooked to the Internet. Although network security is a DIW component (whereas this thesis is focused mainly on OIW), an understanding of the defenses is necessary to effectively break them. Although no network can ever be totally secure, effective steps can, and should, be taken. Network security is more than a series of techniques; it is a state of mind that must be cultivated and maintained.

Any network that wants to protect itself from unauthorized access needs to have safeguards in place to keep out unwanted users. One way to do that is by use of a firewall. A firewall serves as a filter to keep unwanted users and unwanted traffic out of the network.[Ref. 29] It is basically an added layer (or layers) in the security structure. Of course, no firewall is perfect and firewalls themselves are vulnerable. In fact, while a firewall may stop or slow down

a hacker, those efforts can be directed against the firewall as well. If the firewall goes down, external network activity could cease altogether. Of course, this scenario presents a whole new set of problems which must be dealt with.[Ref. 59]

Firewalls are not the ultimate security tool (a common misperception). One could say that a firewall can be seen as something with "a hard, crunchy outside with a soft chewy center". In other words, they offer a false sense of security, because, they, too are vulnerable.[Ref. 60] They may be set up to prevent certain types of traffic (*e.g.*, unauthorized e-mail) while they offer very little protection from other problems (*e.g.*, viruses).[Ref. 61] Also, while firewalls may prevent intrusion, they may also limit functionality of the network by imposing additional restrictions on the users.[Ref. 29]

Numerous firewall products are easily available in the commercial market. In fact, the Internet is often a good source for finding vendors of such products, including composite lists of product overviews and addresses [Ref. 62] One example of such a firewall tool is Black Hole. Black Hole is a product of a Canadian company called Milkyway Networks, Inc. (which currently controls seventy percent of the network security environment in Canada). It is used to prevent unauthorized access to a network in general, especially to sensitive information such as accounting data.[Ref. 63]

Once a user gains access to the network, an authentication process must occur to ensure the user is valid. Traditionally, this has been done via use of passwords and related techniques. Of course, this information must also be protected in order to be effective. If a perpetrator gains access to either the password database or is able to crack individual passwords, then the network is compromised. Often, users facilitate this by choosing easily guessable or

crackable passwords. Ways to improve this process include use of one-time or frequently changing passwords as well as a process for ensuring chosen passwords are "good". Also, the passwords must be adequately protected from compromise.[Ref. 29]

Newer authentication techniques are also emerging. One example is an individual user card, similar to a credit card or a bank card (*e.g.*, the Fortezza card). This card contains all essential user information and must be inserted and validated prior to being given access to the network. While this improves security substantially (a perpetrator must gain physical possession of a card or bypass the enabling software), it is not foolproof. Another, and much more reliable technique is a biometric verification. This involves the use of a physical authentication process unique to every user, such as a fingerprint or retina scan. The future will show an increased use of these more secure techniques (cards and biometrics), especially as the associated costs decline.[Ref. 29]

A final network security technique is encryption. Encryption can occur in basically two different ways: on-line (encryption occurs just prior to transmission) or off-line (encryption occurs shortly after material is composed and before transmission). The two main types of on-line encryption are end-to-end (encryption occurs once) and link (encryption occurs several times along the transmission path). Off-line encryption deals mainly with local encryption of, for example, password files.[Ref. 47]

Essential to understanding any kind of encryption technique or specific product is a knowledge of the key systems involved. A key is basically the mechanism (hardware, software, or both) whereby the encrypted transmission is decrypted. Keys can be either private (where both parties use the same key) or public. In the public key scheme, each party has two keys: a

private one (which should never be shared) and another one that is made available to other users. Both keys are needed to encrypt and decrypt a message. A concept related to the public key system is key escrow. Key escrow trusts a neutral third party (the escrow agent) with part of the key. The escrow agent would only surrender their key when asked to by the parties involved or when dictated by court order. The legal ramifications of key escrow are great and thus are topics of considerable controversy. Several different encryption tools, focused mainly on electronic mail, are available. These include: RSA (Rivest, Shamir, and Adleman), Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP), Digital Encryption Standard (DES), Public Key Cryptography Standard (PKCS), Kerberos, S/MIME (Secure Multimedia Internet Mail Extensions), SKIPJACK, etc. Details of each of these techniques (and others) can be found in any number of sources, some of which are included in the Bibliography.[Refs. 29 and 64]

Perhaps the most critical factors in effective network security are a realization of the problem and education. When coupled with user-unique encryption and verification techniques (such as the highly successful and relatively new Fortezza card), near total (absolute total is never possible) integrity of a network is possible. An effective training program, where users at all levels are taught proper precautions, practical use, and timely incident reporting procedures, is essential. Some form of effective enforcement (*e.g.*, fines or disciplinary action) must also be established to ensure users remain vigilant. Regular (but not predictable) drills should also be held to ensure compliance and facilitate development of security consciousness. Such drills should be implemented by a third party so that effective training is also conducted for network administrators. Only by changing the mindset of all users and administrative personnel can near total network integrity be maintained.

c. Miscellaneous

Several other technologies and processes are also worth mentioning briefly. Miniaturization is a key feature of today's technological developments. While the push is towards more power and capability, such developments must also be smaller and more lightweight. Portability is also a key feature of emerging technologies, in anything from computers to cellular phones. This requires use of new materials and processes to develop long-lasting and reliable batteries (or other power generation schemes) so that the technologies can be effectively employed. Miniaturization and portability facilitates the use of Information Warfare down to the individual user level if necessary. A final area of consideration in the current technology domain is that of simulation. Shrinking budgets dictate innovative training techniques. Highly developed technologies allow for relatively cheap and effective training. Perhaps the most vivid example is the rapid proliferation of virtual reality (VR). VR training is quickly becoming a mainstay for training in many different domains (commercial, industry, military, etc.). Of course, these technologies can also be exploited, as will be discussed in the following chapter.

4. Emerging Technologies

A final category in the description of enabling technologies are emerging technologies. This category includes not only non-traditional types that represent the future of technology and warfighting (*e.g.*, neural networks, artificial intelligence, etc.) but also new uses or extensions of emerging technologies (*e.g.*, wireless networks, Switched Multi-megabit Data Service, Fiber-optic Link Around the Globe, etc.). Two main groupings in this category can be viewed: network functions and cognitive technologies. Several other areas could also be addressed (*e.g.*,

emergence of new materials for construction and manufacturing). While important, the nature of this thesis precludes an in-depth (or even cursory) look at every technological possibility.

a. Network Functions

As the networked world emerges as the *status quo*, technology is focusing on new and improved ways to transmit information quicker and more efficiently. Several technologies that should be included in this category are: Switched Multi-megabit Data Service (SMDS), Asynchronous Transfer Mode (ATM), and Synchronous Optical Network (SONET). SMDS is "a high speed (1.544M and 45M bps), connectionless, public packet switched service that can provide LAN-like performance and features over a metropolitan area."[Ref. 47] SMDS uses the existing telephone infrastructure and the cell relay technique[10] to provide high data rates in a given geographic area. ATM is a similar cell relay technology with speeds from 45 Mbps to 600 Mbps [Ref. 46]. SMDS and ATM offer greater flexibility in that a message can be split up and sent over any number of different paths, thus increasing chances of receipt, even if some parts of a network are down.[Ref. 29] SONET is a fiber optics technology (thus requiring installation of a fiber infrastructure) that offers extremely high data rates, from 51.8 Mbps to 2.4 Gbps [Refs. 46 and 47], as well as the advantages of fiber (see section B2a(4) in this chapter). In each case, data is transmitted faster in a more complicated manner. This provides opportunities and vulnerabilities in both OIW and DIW.

Extensions of new technology are also leading to the creation of new infrastructures. One prominent example of this is the Fiber-optic Link Around the Globe

---

[10] Cell relay uses fixed length "cells" that are transmitted individually and then reassembled at the receiving end. Cell relay is faster than its competitor, frame relay.[Ref. 48]

(FLAG). FLAG is a project which, when completed in 1997, will link Great Britain and Japan with a 27,300 km undersea fiber optics link. This system will have landing points in Spain, Italy, Egypt, United Arab Emirates, India, Malaysia, Thailand, Hong Kong, China, and Korea. The fiber optics link will carry data at a rate of 5.3 Gbps which will be parsed into 120,000 VGCs.[Ref. 65] This innovative project provides enormous potential for Information Warfare. In fact, FLAG could serve as an entry point for IW operations.

b. Cognitive Technologies

The second major division of emerging technology lies in the realm of cognitive technologies. Cognitive technologies include such things as artificial intelligence and neural networks. They represent perhaps the area of greatest growth in the technology domain and perhaps the field which holds the greatest potential for Information Warfare. Since one key aspect in any war is getting inside the enemy's mind and wreaking havoc, the marriage of cognitive technologies and IW present a very formidable weapon.

One powerful example of a cognitive technology is the neural network. It is a computer adaptation modeled after the human brain. Whereas traditional processing connections on networks are often limited to 10 or 20 nodes, neural networks take advantage of the human brain model which allows for connections of tens of thousands of nodes. These nodes operate in parallel (recall the section earlier on parallel computers) so the number of nodes does not impinge on processing time (but a large amount of memory is needed). The power behind neural networks is that their massive processing power enables them to "learn". This is accomplished by assignment of error codes which, after repeated trials, diminish and thus "learning" has occurred. Neural networks can be used for signal processing (classic EW), pattern and image

recognition, speech and language processing, decision making systems, and a myriad of other tasks. The IW application for neural networks is enormous. They could be used for such things as automated decision making and massive data crunching. They can also present an OIW challenge that relies more on an understanding of biology and physiology than on computers (*i.e.*, a neural network can be attacked as if it were a human brain).[Ref. 40]

C. THE POWER OF TECHNOLOGY

In summary, there are a wide range of technologies that can be used in Information Warfare in any number of ways. Technology is a dynamic science that is constantly changing and thus new potentials are developed everyday. Of course, no single discussion of IW enabling technologies can ever be comprehensive or complete. The discussion that has been offered here, and is summarized in Table 8, is but the tip of an iceberg. Yet, this tip offers insight into some ways that some technologies can be used in IW. It should also show the reader that Information Warfare, in its most powerful form, cannot be divorced from technology.

CATEGORY	SUBCATEGORY	EXAMPLES
Computers & Networks	Computer Advances	Parallel computing, Desktop VTC
	Networks	Lotus Notes Suite
	Internet	Java
	Architectures	GII, NII, DII
Telecommunications	Traditional	ISDN, Microwave, Fiber
	Satellite	GBS, VSAT, INMARSAT
	Cellular	PCS, Iridium, GSM
Other Pertinent Technologies	Sensors and Space	Visual, Near-Visual, Optical
	Security	Fortezza, Black Hole, Firewalls
	Miscellaneous	Miniaturization, Energy Tech.
Emerging Technologies	Network Functions	Wireless, FLAG, SONET, ATM
	Cognitive Technologies	Neural Networks, AI

Table 8. Enabling Information Warfare Technologies.

V. OFFENSIVE INFORMATION WARFARE

The first four chapters of this thesis have focused primarily on Information Warfare from a broad perspective. The tough issue of definitions, an overview of the organizations involved, and a brief look at some of the enabling technologies have all been examined. To gain further insight into the usefulness of Information Warfare, a decision must be made for further exploration.

What should be obvious to the reader by now is that IW is so large a field of study that no single document could fully cover all of its facets. As a result, any study must be partitioned into manageable pieces. This remainder of this thesis will examine the partition of Offensive Information Warfare. Two caveats should be noted, however. First, OIW and DIW are complementary; one cannot be divorced from the other. While recognizing this fact, OIW will be the primary focus for the remainder of the thesis. Second, an understanding of the concepts presented in Chapters II through IV are critical to understanding the ensuing discussion of OIW.

A. RATIONALE FOR OFFENSIVE INFORMATION WARFARE

1. Engaging In Offensive Information Warfare

The first question that should come to mind is: should the United States engage in Offensive Information Warfare? There are numerous political, economical, social and legal issues that surround OIW. A discussion of most of these issues is reserved for Chapter VII. However, the emergence of IW as a definite part of warfare into the foreseeable future demands that the United States be prepared to execute an effective IW plan, both offensive and defensive,

on short notice. Therefore, the requirement exists to make those preparations. Of course, the time to make such plans is prior to the commencement of hostilities.

This chapter will illustrate some of the ways that OIW could be conducted. Unfortunately, the majority of OIW efforts and endeavors inside the U.S. government are highly classified. As a result, this chapter will not contain any specific programs or projects that may exist in the OIW realm. However, such knowledge is not critical to a basic understanding of OIW concepts and tools. All of the ideas presented here are drawn from open source material or are derivations thereof. By no means should they be interpreted as components of a U.S. government OIW plan. They merely present possibilities that could be applied when conducting an OIW campaign. Of course, the tools and concepts presented here are by no means comprehensive; numerous others do exist and should be examined. This chapter is meant to paint a picture of OIW in general.

2. "Defining" Offensive Information Warfare

Chapter II focused on the problem of trying to define Information Warfare. Trying to pin a tangible definition on something so large and ubiquitous as Information Warfare is futile. The end result of Chapter II was the settlement on Paradigm F as a working definition or context for this thesis. Inherent to that "definition" was the fact that IW can be both offensive and defensive in nature; several uses of each have been cited in all of the chapters so far. Still, in order to discuss OIW effectively, it must be bounded. For the purposes of this thesis, Offensive Information Warfare can be defined as: any action taken to degrade or destroy an enemy's information infrastructure and systems. No attempts will be made to define what comprises this "infrastructure" until the following chapter. Instead, this chapter will focus on some tools.

The potential for OIW as a decisive battlespace force multiplier is enormous. Any or all aspects of a given society, from military to commercial, can be brought to its knees by effective use of OIW. A caveat to that argument is that such a society must be information-dependent (using OIW against a non-information-dependent society or nation is explored further in Chapter VII). OIW can be used to achieve hard or soft kills that are subtle or blatant. Technology is a major driving force in achieving this diversity. OIW can force an enemy to capitulate without the loss of a single human life.[Ref. 66]

3. Creating An Offensive Information Warfare Strategy

Of course, in order to be useful, OIW must be applied in a structured fashion. In keeping with that goal, Figure 6 represents a flowchart for an OIW Strategy that has been devised by the Office of the Secretary of Defense (OSD).[Ref. 13]

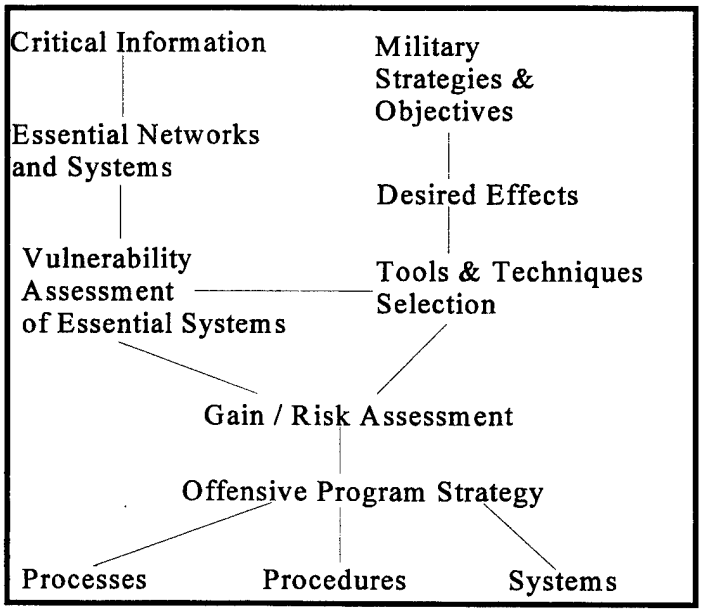

Figure 6. OIW Strategy Flowchart.[From Ref. 13]

Since this figure will be referred to periodically throughout the rest of this thesis, a brief explanation is necessary. Starting in the top left corner, there is the entry entitled "Critical Information". This is information which the enemy is dependent upon for a given system or infrastructure. This information feeds into the "Essential Networks and Systems" step which is self-explanatory. Friendly forces need to identify weaknesses in those systems, which is the next step, "Vulnerability Assessment". Concurrently, along the right side of the figure are the friendly "Military Strategies & Objectives". Recall from Chapters II and III that such guidance is sporadic at best today. From that step is derived the "Desired Effect" (*i.e.*, what we want to do to the enemy). From there, the appropriate "Tools & Techniques Selection" must be made. Notice that these tools and techniques are directly tied into the results of the "Vulnerability Assessment" step (obviously). From there, the two tracks merge into a "Gain/Risk Assessment" where the merits of a given plan are analyzed and weighed against the possible drawbacks. The next step is the formation of an "Offensive Program Strategy". Finally, the required "Processes", "Procedures", and "Systems" are promulgated.[Ref. 13]

In the context of Figure 6, this chapter is concerned primarily with the "Tools & Techniques" portion. Some discussion will be made about "Desired Effects." The first three steps on the left side of the drawing will be discussed in more detail in Chapters VI and VII. Some discussion has been made of "Military Strategies & Objectives"; any specifics in this regard would most likely be highly classified and thus beyond the scope of this thesis. Some brief discussions on the other steps in the figure will be touched upon in subsequent chapters.

4. Revisiting Centers of Gravity

One should recall from Chapter I the discussion on Centers of Gravity (COGs). They are essentially the weak links which, if exploited convincingly, lead to the desired results in a given campaign. John Warden has often been credited with the "Five Strategic Rings Theory"[Ref. 67] in which he places COGs in five concentric rings. The outermost ring contains the military forces while the innermost ring is the leadership element. Traditionally, these rings generally had to be attacked in succession from outside in. OIW changes that mentality by allowing a direct attack on the innermost ring without (possibly) affecting any other ring.[Ref. 68] The paradigm shift to Third Wave mentality is the reason. Now, Offensive Information Warfare permits "global disruption of critical command and control networks, which are the centers of gravity of modern militaries"[Ref. 66] Thus, identifying COGs is critical to success, and they play directly into several aspects of the OIW Strategy depicted in Figure 6 ("Military Strategies & Objectives", "Desired Effects", and "Vulnerability Assessment," at a minimum).

5. Examining Targets Sets For Offensive IW

Offensive Information Warfare demands a new approach towards developing target sets. As mentioned in the discussion of COGs, finding the "soft underbelly" of the enemy can be accomplished in whole new ways. OIW targets should be selected for their epistemological value in undermining enemy COGs. Epistemology means "everything a human organism--an individual or a group--holds to be true or real, no matter whether that which is held to be true or real was acquired as knowledge or as a belief".[Ref. 69] In other words, target sets now include COGs that are focused on human thought processes and perceptions. This is a radical change from many traditional forms of warfare, and it is the source of much controversy. The reader

should take a moment to dwell on the epistemological paradigm. It brings with it a startling new approach to warfighting. Friendly forces can influence the enemy's thoughts and ideals, down to even the basic core of their existence as a society or a people, without them even being aware of what is happening! These are very profound and very powerful concepts! Therefore, target sets for OIW extend beyond traditional boundaries to include such things as political and economic systems.[Ref. 68]

B. OFFENSIVE INFORMATION WARFARE TOOLS AND TECHNIQUES

Perhaps the best way to demonstrate Offensive Information Warfare is to examine some of the tools and techniques that could be used to execute it. For the purpose of this discussion, these tools and techniques are grouped into four categories based on the form involved : Traditional Forms, Phreaking Forms, Computer Enabled/Dependent Forms, and Technology Enabled/ Dependent Forms. Each of these categories has subcategories with some specific examples of the types of things that could be employed in waging OIW. Keep in mind that these tools and techniques are all drawn from open sources. Some work effectively, some may not work at all, some may not even exist yet, and some other tools or techniques may have (almost definitely have) been omitted. By no means does the mentioning of a specific tool or technique imply that the U.S. government or U.S. military could or would use such weapons, or that they even possess them; the items mentioned here are only possibilities for using OIW in a battlespace.

1. Traditional Forms

The first major category of OIW tools and techniques are Traditional Forms. Traditional Forms are those that have been used in previous types of warfare. The major difference is that the targets have changed, as discussed above. Also, new technologies or tactics may enhance old forms of warfare to give them more of an edge in the IW domain.

a. Physical Destruction

Physical destruction, a sub-component of Command and Control Warfare (C2W), is fairly self-explanatory. It involves the use of anything from iron bombs and precision-guided munitions (PGMs) to artillery and special forces units. The targets are Information Warfare-type targets, such as command centers, telephone switches, or microwave towers. Many would consider physical destruction as a borderline OIW weapon, at best. There is a large school that believes blowing up something is not Information Warfare. On the contrary, it is indeed IW if it achieves the intended epistemological goal.

b. Electronic Warfare

Electronic Warfare (EW), like physical destruction, is another C2W pillar that has been around a while. It involves the use of such traditional means as jamming, again focused on a different (perhaps) target set. EW as an OIW weapon also means exploiting technology in new fashions. One example of this is the Van Eck detector, which is essentially an electronic eavesdropper. Computers and other electronic devices emit electromagnetic radiation. This radiation can be picked up by devices called Van Eck detectors.[Ref. 70] This device could potentially be used for such things as capturing keyboard keystrokes [Ref. 71] which could, in turn, be used to figure out passwords for future attacks.

c. Information/Intelligence Collection

Information or Intelligence Collection has been a part of warfare since the dawn of time. Timely intelligence and accurate information have always been critical to success in conflict. Thus, warfare in the Information Age is no different. However, new technologies (many discussed in the previous chapter) and tactics mean new dimensions for this technique. An example is the age-old trick of "dumpster diving" or "waste archeology". This, of course, involves poring through the enemy's trash in the hopes of garnering needed information or intelligence. In the Information Age, dumpster divers are looking for such things as carelessly tossed passwords on yellow stickies or printouts of network activity.[Ref. 72]

d. Psychological Operations

Psychological operations (PSYOPS) are yet a third piece of the C2W structure, yet an important one for gaining the epistemological advantage. PSYOPS include such things as propaganda broadcasts from aircraft (such as occurred in Haiti and Panama). The Information Age also means using new dissemination methods, such as the Internet to broadcast PSYOP messages.[Ref. 73] Three additional PSYOP tools require further mentioning: the mass media, video morphing, and voice synthesis.

(1) The Media. The media has always had a role to play in psychological operations, be it a radio broadcast, newspaper, or television news show. However, a proliferation of technology coupled with a world that is increasingly relying on television for information, presents a formidable PSYOP weapon. Emerging technologies, such as the Direct Broadcast System (DBS) discussed in Chapter IV, allow for the transmission of large amounts of video data in a very short time. Such broadcasts could be tailored to paint a picture that friendly forces

want to project to the enemy (not necessarily a true picture) to gain the mental advantage. A prime weapon for this task could be the Cable News Network (CNN). This almost worldwide news station prides itself on timely communication of breaking news. By using misinformation, along with specially prepared audio and video clips, friendly forces could make enemy forces or even the enemy's homefront believe something is happening that is, in reality, not.[Ref. 30]

For example, a special news segment about enemy atrocities (which never actually occurred), complete with pictures of dead children (computer generated, of course) is aired over CNN only to stations in the enemy's homeland (by special prior arrangement with CNN). The people at large lose faith in their leaders, and the enemy is forced to cease hostilities. Of course, this scenario raises more than one moral and ethical issue, which need to be considered (such issues are addressed in Chapter VIII).

(2) Video Morphing. The scenario just presented calls into question yet another PSYOP technique, video morphing. Video morphing involves transforming one or more video images, such a news clip, in order to distort reality. This was done several times with a high degree of success in the movie *Forrest Gump*.[Ref. 70] By taking this process one step further, the result is the scenario shown above.

(3) Voice Synthesis. A final example of a PSYOP technique is voice synthesis. This procedure involves artificially creating a voice by use of a computer in order to emulate a desired voice, an enemy leader for example. This synthesized voice could then be used to create a propaganda message for example (perhaps it could be the accompanying audio clip for the video-morphed news clip described in the scenario above). Again, this weapon involves

several tough issues that must be addressed before it could be fully employed in an information battlespace.[Ref. 74]

2. Phreaking Forms

"Phreaking" is a term that applies to the manipulation of telephone systems for other than their intended purposes. In much the same way that a hacker is concerned with penetration of computer systems, a "phreaker" works with telephone systems. Several additional terms, such as "phracking" are related to this discipline. For the purpose of this thesis, phreaking will be viewed as exploitation of telecommunications systems. There are two basic breakdowns for this category: traditional and cellular, each of which is briefly explained below. The main problems with implementing phreaking technologies are the current legal constraints.

a. Traditional Telecommunications

Phreaking in the traditional telecommunications arena has been ongoing since the advent of telephone systems. This area includes such things as phone taps and redialers, items that law enforcement officials have used almost exclusively in the past. Phreaking also includes (and is perhaps best well-known for) penetration of telephone computer systems for such things as getting free phone calls or altering billing records. Although this latter form of phreaking has historically been performed by amateurs acting under their own motives, the revolution in Information Warfare brings new potential. Now, an organized group could perform the same types of activities under the auspices of an OIW plan. Phone systems could be penetrated in order to monitor network traffic or plant computer viruses or any number of things. A world that relies on telephony to survive is also vulnerable to its weaknesses.

b. Cellular Communications

A newer field of study that is emerging is phreaking of cellular systems. Cellular systems have always been vulnerable. Some of those vulnerabilities were explored in the previous chapter. Electronic Serial Numbers (ESNs) can be captured. Not only could this trapping lead to fraudulent charges, it could also be exploited for transmission of, for example, voice synthesis attacks as discussed above. The evolution of networked computer systems operated by cellular technology (recall the discussion on wireless networks and PCS in Chapter IV) will require an increasing emphasis on OIW techniques for cellular systems.

3. Computer Enabled/Dependent Forms

The Third Wave revolution has brought with it a heightened reliance on technology. In fact, this technology explosion has been a major enabler for the birth of modern Information Warfare. Perhaps the greatest such explosions have occurred in the area of computer advances. In fact, perhaps the most powerful weapon for those who would wage Information Warfare is the computer. This category is essentially broken into two groupings: Malicious Software [Ref. 70] (concerned with attacks on software) and Hacking (concerned with attacks on systems).

a. Malicious Software

The first subcategory is Malicious Software. This form of IW is perhaps the most visible and prolific to the individual user. In fact, one would be hard-pressed to find a veteran computer user that has not dealt with at least one of the software components discussed below. While such tools have customarily been used by individuals for accomplishing self-centered goals, the OIW potential for an organized, yet essentially hands-off, campaign is enormous.

(1) Viruses. Perhaps the best known software weapon is the virus. A computer virus can perhaps best be described as "a code fragment that copies itself into a larger program, modifying that program. A virus executes only when its host program begins to run. The virus then replicates itself, infecting other programs as it reproduces."[Refs. 25 and 75] These executed code fragments then modify or destroy other data in the computer. Maybe the virus even drains the computer's resources to the extent that routine tasks are almost impossible to perform.[Ref. 76] There are innumerable viruses in existence. They proliferate over such media as the Internet (*i.e.*, someone downloads an infected program, sends it a friend, etc.).

An example of a coordinated OIW virus attack might be posting an infected story on the CNN home page on the Internet. Intelligence assets report that the staff of the enemy dictator routinely downloads stories from the CNN page to prepare daily briefings. The infected story is incorporated into the briefing, which is on a floppy disk that is then passed among several staff members for editing. Along the way, the virus infects each computer it passes through. Finally, it reaches the dictator's computer where the brief is reviewed by the dictator's aide; that computer, too, becomes infected. Shortly thereafter, the dictator's command post is scrambling; for some inexplicable reason, all of the staff's hard drives erased themselves. Another successful OIW attack is complete... As a side note, there are various legal problems that preclude this scenario from being implemented today (some of which will be discussed in Chapter VIII).

(2) Trojan Horses. A Trojan Horse is very similar to a computer virus. The major difference is that a Trojan Horse is non-replicating.[Ref. 77] The end result with both viruses and Trojan Horses is the same: data on a computer is altered, degraded, or destroyed.

However, the utility of a Trojan Horse is limited in that it cannot replicate itself. Therefore, each computer would have to be infected individually. Of course, that could be accomplished in a software upgrade. For example, Country X arranges for a neutral third party (which is under contract from Country Y to produce a software upgrade to their military operating systems) to interject a Trojan Horse into the software. Country Y installs the software, and the Trojan Horses executes, deleting the computers' hard drives. Again, there are more legal problems, but otherwise, the capabilities exist.

(3) Logic Bombs. Yet another related tool is the logic bomb. A logic bomb is similar to a Trojan Horse, except that it is conditionally executed.[Ref. 76] For example, a logic bomb could be used to coordinate an OIW strike. Taking the Trojan Horse scenario one step further, logic bombs could be inserted into a software upgrade to an early warning system. They would be scheduled to execute at a pre-determined time in conjunction with an airstrike. When the airstrike occurs, the computers controlling the enemy's search radars inexplicably shut down...

(4) Worms. A final type of malicious software tool is the worm. Worms are programs that "reproduce" by copying themselves over and over. They spread from computer to computer via networks.[Ref. 76] Their mission is primarily to drain computer system resources. Historically, worms have not been used to modify or destroy data, although they technically could be used for that purpose.[Ref. 25]

b. Hacking

The second major subcategory of the Computer Enabled/Dependent Forms category is Hacking. As mentioned before, this definition of "hacking" is meant to convey a

systemic attack vice a software one. There are any number of tools and techniques that fall into this subcategory. Eight of them are discussed here: Data Manipulation, Sniffers, Probes/Mapping, Crackers, Spoofing, Hijacks, Back Doors, and Denial of Service (DOS) attacks.

(1) Data Manipulation. When one thinks of the stereotypical hacker at work, one thinks of the data manipulation technique. Someone sits down in front of a computer and gains access to a target system (by any number of means, some of which are discussed herein). Once "inside" the system, that person then modifies, creates, or destroys data to achieve a goal. In the past, these goals have generally been limited to that individual. However, the advent of IW as a warfare discipline advances the theory for an organization to perform coordinated data manipulation attacks on adversary systems.

(2) Sniffers. A sniffer is a "network monitoring tool that enters a system and detects up to the first 120 keystrokes of a newly opened Internet session, capturing a user's host, account and password information."[Ref. 78] A sniffer is a powerful tool, in that it can be the "foot in the door" for a series of OIW attacks. Sniffers are easily available (they are prolific on the Internet, for example). They are also automated, so they can monitor large amounts of network traffic. These sniffers are disguised as legitimate network tools. As more and more passwords, etc., are trapped, more holes are opened up on that network (and perhaps other connected networks as well).[Ref. 79] The end result could be almost total control of an adversary's networks. If concealed properly, sniffers could form the "reconnaissance" phase of an OIW campaign. From there, a striking force could gain valuable insight into the enemy's routine, organization, etc.

(3) Probes/Mapping. A third type of Hacking tools is probes. Probes are tools that are used to map out a network. One of the best all-encompassing definitions on probes comes from an pseudo-anonymous posting to an Internet mailing list which says that a probe is

> [A]n artificial life form that exists only electronically and on storage media and uses artificial intelligence to accomplish its mission. Its mission is to map networked systems, steal and internally store copies of sensitive files and at some point to return to its point of origin. As it traverses the network, it stores a map of the network in a heap [a form of binary tree which can be quickly and logically searched] structure. If network links dropped or were taken down on the path the probe would follow back, it can search the heap to find another way home.[Ref. 80]

This somewhat lengthy definition is very good. It explains the purpose of a probe as well as its technology basis (recall the discussion of artificial intelligence in the previous chapter). As one can see from the definition, probes are highly sophisticated and very powerful tools. Once access is gained to an enemy's network, a probe could be inserted to either perform reconnaissance or attacks or both. The main problem for the probe would appear to be remaining hidden.

(4) Crackers. Cracking is the process by which a software tool attempts to gain access to a system by "guessing" passwords. The variables in this process are the length of the passwords, the types of passwords (alphanumeric, case sensitive, special characters, etc.), and time. Given enough time and a powerful enough computer and software, almost any password can be guessed. In fact, 25% of all passwords are easily cracked. The time required to crack any password is a linear function based on the total number of password combinations and the length of the password and assuming that each "guess" requires the same amount of processing time (approximately one millisecond).[Ref. 81]

(5) Spoofing. Spoofing is the ability of one computer system user to impersonate another user. This is accomplished by impersonating that person's computer's Internet Protocol (IP) address. The system that is being attacked believes that the spoofer is a trusted user.[Ref. 82] This process is often simplified by the fact that IP addresses for many machines are arranged in a logical sequence.[Ref. 81] Once trusted access is obtained, any of a number of OIW attack tools and techniques can be utilized (*e.g.*, data manipulation, insertion of viruses, Trojan Horses, or worms, etc.). Spoofing attacks are difficult to detect because most network monitoring programs do not check the incoming routers for source IP addresses, only destination ones.[Ref. 82]

(6) Hijacks. Another OIW technique is the hijacked session (or hijack for short). In this method, a perpetrator gains "root" (most privileged) access (perhaps through something such as cracking or sniffing) of a machine or system. He or she then uses that root access to take control of another existing user session. The hijacker then has control of that user's account (the victim may or may not be aware). If the victim has remotely accessed another computer, the hijacker may have access to that remote system as well, without any kind of authentication procedure.[Ref. 82]

(7) Back Doors. Another Hacking tool is the back door or the trap door. A back door is a security "loophole" in a piece of software that is put in place by the designing programmer. This loophole provides a means of entry back into that program at a later date.[Ref. 25] Recalling the scenario depicted under the Trojan Horse section earlier, the software upgrades sold by the intermediary country could be designed with trap doors. In fact, perhaps the

designers could be bribed (not an unheard-of concept) by Country X into revealing the access technique. Now Country X has a means to penetrate Country Y's systems.

(8) Denial of Service. A final Hacking technique is Denial of Service (DOS). The purpose of a DOS attack is to overwhelm the defenses of a victim's computer network system. This is accomplished by, for example, sending a continuous stream of large electronic mail messages to the victim's address. Such a loading soon inundates the victim's system. The victim would then be forced to make a decision to cease receipt of all message traffic (including possibly critical information from another valid user) or not.[Ref. 83] While the system is trying to handle the volume of traffic, perhaps the perpetrator tries to gain access to other parts of the victim's system while using the DOS attack to mask the intrusion. One drawback to the DOS technique is that cannot be hidden (although the origin of the attack can be hidden, perhaps through something such as an anonymous remailer[Ref. 84]).

4. Technology Enabled/Dependent Forms

The final category of OIW attack tools and techniques is Technology Enabled/Dependent Forms. While may of the items discussed so far rely heavily on technology, this category is reserved for those weapons that depend almost exclusively upon technological developments. In fact, in almost every case listed below, the methods for these attacks have not been perfected or proven. They represent the "cutting edge" of Offensive Information Warfare weaponry. Many of these items may appear to be extracted from a science fiction novel. While the details may not have been perfected, the ideas are at least feasible, given today's technology.

a. Chipping

The first tactic to be discussed is chipping. Chipping is "the practice of making electronic chips vulnerable to destruction by designing in weaknesses".[Ref. 70] This weakness then comes to light at a pre-determined time or when a pre-determined condition is met.[Ref. 26] For example, Country X knows that its potential adversary, Country Y, buys the computer hardware for its shipboard air defense systems from Country Z. As luck would have it, Country Z buys its computer raw materials (such as semiconductors) from Country X. Therefore, Country X specially designs the computer chips (*i.e.* it "chips" them) in view of a potential crisis (unbeknownst to both Countries Y and Z). The resulting computers that Country Z sells to Country Y have been "chipped". In fact, they have been designed to activate upon receipt of a signal transmitted by Country X. Several years later, Country X launches a pre-emptive air strike at a naval task force belonging to Country Y. The inbound air raid transmits the trigger signal. Suddenly, all of the task force's air defense computers shut down on an unexplained hardware failure... This scenario is, of course a very elaborate one, but it is only one of countless chipping possibilities.

b. Energy Weapons

Energy weapons are the second subcategory of Technology Enabled/Dependent Forms. Three examples of these science fiction-type weapons are: High Energy Radio Frequency (HERF) guns, Electromagnetic Pulse (EMP) bombs, and High Power Microwave (HPM) weapons. A brief description of the function of each is included below. The target for each weapon is electronic equipment, such as computers. Energy weapons could be very controversial, in that they could harm humans as well as electronics.

(1) HERF Guns. A HERF gun is essentially a powerful radio transmitter. When activated, it transmits a radio signal at the target. This signal interrupts the normal electron flow pattern. Depending on the power of the transmitted signal and a variety of other factors, the intended targets are either destroyed (components burn up) or degraded (equipment shuts down). HERF guns can penetrate buildings or other structures (unless the buildings are specially designed to withstand the beams).[Refs. 25 and 26]

(2) EMP Bombs. EMP (or EMP/T where the T stands for Transformer) bombs operate on a concept very similar to HERF guns. However, EMP bombs are generally area weapons (whereas HERF guns are directional weapons). Also, EMP bombs tend to be more powerful (on the order of a thousand times or so). The theory behind the EMP bomb is exactly that of the EMP wave released by a nuclear explosion.[Refs. 25 and 26]

(3) HPM Weapons. The final example of an energy weapon is the HPM. HPM's are similar to HERF guns. They transmit an intense radio frequency beam in almost every frequency range (so as to affect almost any type of electronic device). The power of this weapon is on the order of 10 Gigawatts (GW)! In an upcoming book on "Information Terrorism", Paul Strassman outlines the details of such a weapon, include schematics and peak power diagrams. HPMs can also kill or injure people (by literally cooking that person, similar to the way a microwave oven cooks).[Refs. 49, 85, and 86] Naturally, there might be strong objections in some quarters to the use of such a weapon.

c. Microbes

Another type of Technology Enabled/Dependent Forms is the microbe. This is essentially where information warfare meets chemistry and biology. Today, various microbes

have been designed that "eat" oil and are used for oil spill clean-ups. Microbes in an OIW role perform similarly. Specially designed microbes feast on silicon. When introduced into an adversary's electronics systems (the real trick), the microbes devour (and thus destroy) the systems.[Refs. 25 and 70] Naturally, there are ethical and moral issues to contend with, as well as legal ones.

d. Nano Machines

A final example of OIW weapon are nano machines. These devices can probably best be described as

> [T]iny robots (smaller than ants) that could be spread at an information center of the enemy. They crawl through the halls and offices until they find a computer. They are so small that they enter the computer through slots and shut down electronic circuits.[Ref. 25]

Of course, these tiny robots would be networked with one another, communicating their position back to the attacking forces (recall the discussion of the networked battlespace from Chapter I). These robots are also dependent on such technological developments as miniaturization (as mentioned in Chapter IV). That concludes the discussion of specific Offensive Information Warfare tools and techniques. Table 9 summarizes these weapons.

CATEGORY	SUBCATEGORY	EXAMPLES
Traditional Forms	Physical Destruction	Precision Guided Munitions
	Electronic Warfare	Jamming, Van Eck Detection
	Info/Intel Gathering	Dumpster Diving
	Psychological Operations	Media, Video Morphing, Voice Synthesis
Phreaking Forms	Traditional Telecomms	Bugs, Wiretaps
	Cellular Communications	ESN Grabbers
Computer Enabled/Dependent Forms	Malicious Software	Logic Bombs, Trojan Horses, Viruses, Worms
	Hacking	Data Manip., DOS, Sniffers, Probes/Mapping, Crackers, Spoofs, Hijacks, Back Doors
Technology Enabled/Dependent Forms	Chipping	N/A
	Energy Weapons	HERF Guns, EMP Bombs, HPM Weapons
	Microbes	N/A
	Nano Machines	N/A

Table 9. Offensive IW Tools and Techniques.

C. CONSIDERATIONS FOR OFFENSIVE INFORMATION WARFARE

As one can see, there is a plethora of OIW weapons. In OIW, as with any warfare strategy, selecting the right balance of weapons to achieve the desired goal is critical to success. The United States is grappling with how to effectively employ Offensive Information Warfare, or

even if it should. As alluded to previously, there are any number of issues that surround the use of OIW weapons and tactics. Chapter VIII is the focus of the majority of these discussions. This part of the chapter will address a possible partitioning scheme for OIW weaponry as well as some ideas about employment of OIW.

1. Partitioning The Attack Domain

One difficulty in developing a coherent OIW strategy (recall the need for such from Figure 6) is that there are a large number of different types of weapons that could be used. How to use each weapon and in what circumstances would be the object of much discussion. The United States knows how to employ sea, land, and air power because it has been doing so quite convincingly for many years. But what about "info power"? This is a whole new warfighting discipline, which makes the problem that much more difficult.

One possible way to approach the problem is to look at the goals of the attacking force. A different mix of tools and techniques would be employed for a "show of force"-type strategy than would be used in an "all-out info war"-type strategy. One method for facilitating the selection process is by partitioning the attack domain by goal and placing different weapons into that matrix. Then, based on the goals, the right combinations of weapons could be selected.

An example of one possible partitioning scheme is shown in Table 10. Here the major divisions are Covert and Overt, depending on the degree of stealth desired by the attacking force. Under each category are subcategories based on lethality. "Lethality" in the context of this table means lethality to the information systems, not necessarily loss of human life (although that is a very real possibility in some instances). The final column of the table shows the various tools and techniques that could be used for that mission. One should keep in mind that the entries in

this matrix are not absolute; in fact, some weapons, employed differently, could easily transition to another category. This table is only meant to serve as a means to partion the problem into manageable chunks.

CATEGORY	SUBCATEGORY	EXAMPLES
Covert	Lethal	Malicious Software
		Chipping
		Microbes
		Nano Machines
	Non-Lethal	EW (Van Eck Monitoring)
		Info/Intel Collection
		Phreaking (both forms)
		Hacking
		Nano Machines
Overt	Lethal	Physical Destruction
		EW (Jamming)
		Energy Weapons
	Non-Lethal	Psychological Ops., DOS

Table 10. Possible Partioning Scheme For OIW.

2. Using Offensive Information Warfare

Offensive Information Warfare should be considered as a viable weapon in future conflict. The tools exist to perform powerful attacks. In fact, many of those tools are easily available on the Internet. Although the easy access to such tools spurns systems adminstrators to tighten control on their systems, it also spurns creation of more spohisticated weapons. Any number of issues surround the use of OIW: goals of the attacking force, intelligence support, legal/political/ economical/moral ramifications, etc. (all of which are addressed in Chapter VIII).

The bottom line is that IW is here to stay (at least into the forseeable future) and the United States should be prepared to use it.

In fact, IW in an offensive role should be employed by military commanders. A 1994 report by the Defense Science Board states that, from an IW standpoint, military commanders should be able to:

- Manage perceptions of events or circumstances
- Deceive potential adversaries
- Influence information in content or delivery
- Debilitate or destroy information of others
- Protect its interests through INFOSEC [Information Security] or Communications Security (COMSEC) [Ref. 87]

With the exception of the last one, all of these bullets fall directly into the OIW realm. This chapter has examined some of the ways that those tasks might be accomplished, albeit in general terms.

With the need for Offensive Information Warfare recognized, one must now turn to how an adversary could be attacked using some of the tools and techniques described in this chapter. This is the focus of Chapter VII. First, however, some kind of insight is necessary into the kinds of OIW targets that a given country might have. Developing this insight into a somewhat rigorous model is the focus of Chapter VI.

VI. THE INFRASTRUCTURE AND INFORMATION WARFARE

A. THE ROLE OF THE INFRASTRUCTURE

The previous chapter addressed the need for Offensive Information Warfare as well as some of the tools and techniques that could be used to perform that mission. One point that should be evident from that chapter is the need for a specialized target set, one that is epistemologically directed. This chapter will provide one possibility for structuring those target sets. The approach for that structure will be a template focused on the concept of an "infrastructure". Brief descriptions of each component in that template will be accompanied by possible ways that OIW might be used in that context. After the template is explained, the discussion will turn in the following chapter to some considerations and issues that must be addressed when contemplating OIW attacks. First, however, an in-depth look at Centers of Gravity and the need for an infrastructure template are necessary.

1. Centers of Gravity Again

The role of and the need for Centers of Gravity (COGs) in an Information Warfare campaign has been touched upon in Chapters I and V. This chapter will address some of the specifics in determining such COGs. First, however, a somewhat more detailed examination at Centers of Gravity is required.

Centers of Gravity have played an important role in military conflict for almost two centuries. They have become an integral part of U.S. military planning today. The original use of the term is often credited to the great strategist, Carl Von Clausewitz. He stated that COGs are

"the hub of all power and movement, upon which everything depends. That is the point against which all [of] our energies should be directed."[Refs. 9 and 88]

The increasing emphasis on joint operations has also prompted statements on COGs in joint doctrine publications. For example, Joint Publication 3-0 states that "[i]dentification of enemy centers of gravity requires detailed knowledge and understanding of how opponents organize, fight, make decisions, and their physical and psychological strengths and weaknesses."[Refs. 88 and 89] Defining and exploiting some of those strengths and weaknesses are central concepts in this chapter.

The determination of COGs as defined in Joint Publication 3-0 requires the use of a convenient, yet powerful model. An example of such a model is the Warden Five Rings Model (which was introduced in the previous chapter). With this model, the enemy is seen as a system that can be broken down into five components, organized as concentric rings. Figure 7 is a visual representation of this model. The innermost ring is considered the most vital to the enemy.

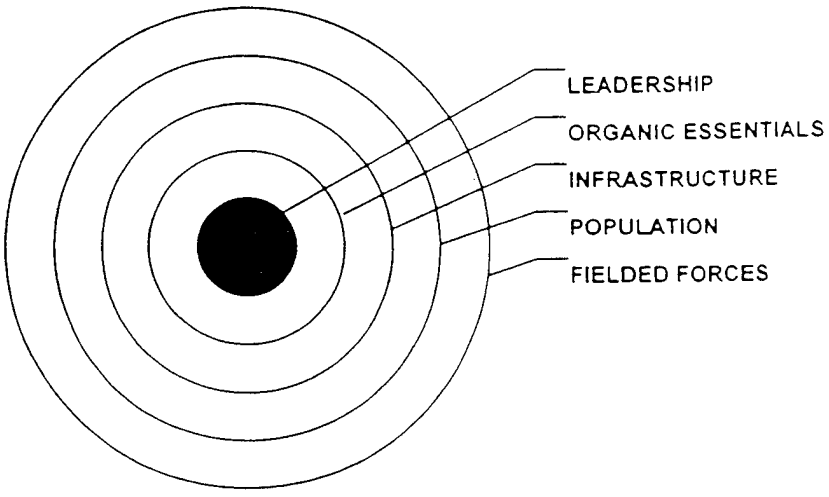

Figure 7. Warden's Five Rings Theory [From Ref. 90].

The rings then decrease in relative importance moving from the center outward. Historically, these rings have generally been attacked from the outermost ring (Fielded Forces). Starting with the Gulf War, the outermost ring was mostly bypassed and other rings (most notably the Leadership ring) were attacked. Information Warfare allows for simultaneous attack of some or all of these rings (with possibly more effectiveness than a conventional attack).

These last few paragraphs have shown that COGs are essential in warfare and they should target specific items *(i.e.*, leadership, infrastructure, physical and psychological strengths and weaknesses, etc.). These needs tie directly into the Offensive Information Warfare Strategy developed in the last chapter. For ease of review, that diagram is reprinted below as Figure 8.

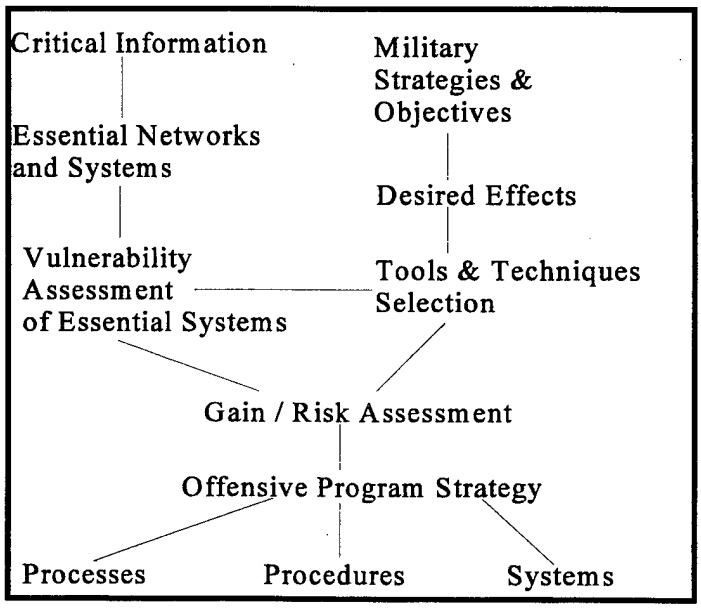

Figure 8. OIW Strategy Flowchart.[From Ref. 13]

COGs have a role in at least the top half of the diagram. Identifying critical information as well as the vulnerabilities of networks and systems is essentially the determination of Centers of Gravity.

2. The Need For A Template

If Centers of Gravity are to be developed and exploited in an Information Warfare domain, some kind of utility must be developed to facilitate this process. Perhaps one approach is to first consider the IW environment. Figure 9 is one possible depiction of the Information Warfare Battlespace. Several key elements of Paradigm F (the context of IW for the purpose of this thesis, developed in Chapter II) can be seen here: C2W is a sub-set of IW, IW occurs at all levels of war, from strategic to tactical, etc. One interesting additional feature is the series of vertical bars denoting various infrastructures: political, economic, physical, and military.

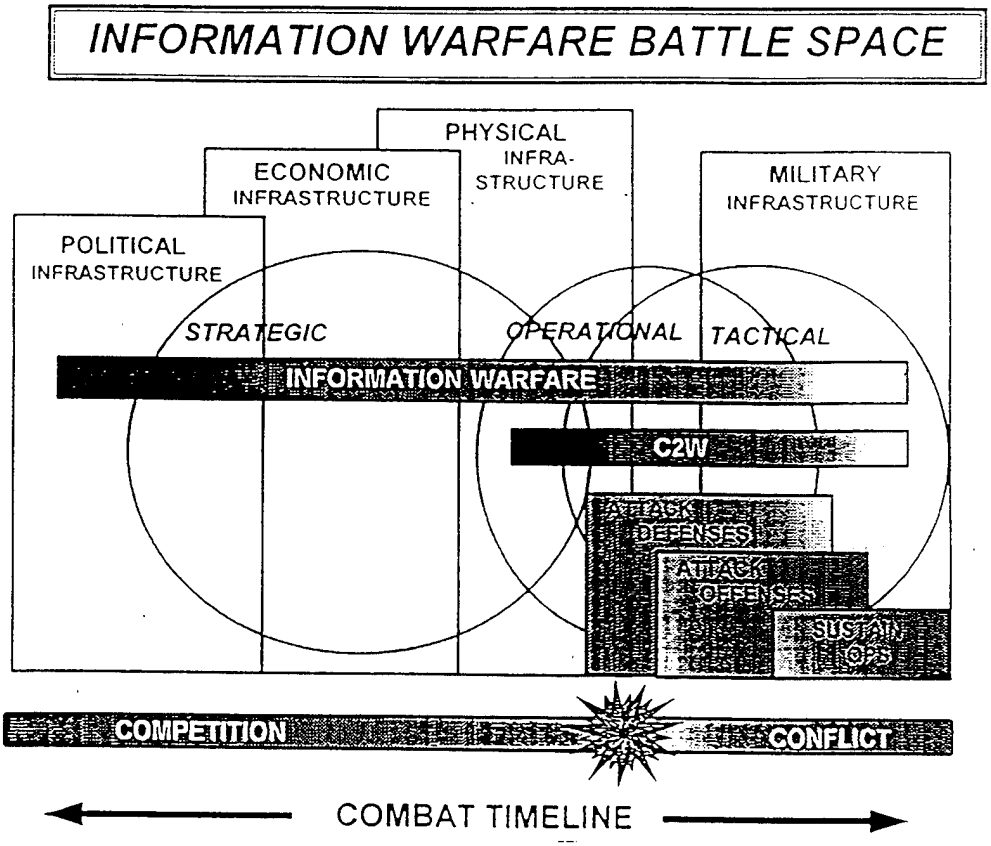

Figure 9. Information Warfare Battlespace.[From Ref. 32]

Using the Warden model and the Joint Publication 3-0 philosophy on COG's, along with the IW Battlespace diagram, a synthesized target domain begins to emerge. Effective Offensive Information Warfare is directed against the enemy's Centers of Gravity. From these COGs, epistemological target sets (as discussed in the previous chapter) are derived. Naturally, choosing those target sets must be done in a structured and useful fashion. This chapter is focused mainly on creating just such a structure.

B. ATTACKING THE INFRASTRUCTURE

Developing a useful template for OIW target sets is not an easy task. As seen in previous discussions, Information Warfare is a large and complex process. It spans all levels of war as well as the whole time line of conflict. OIW target sets require large amounts of detail and precision. Still, any tool that is developed for creating target sets must have some utility. It must be consistent and flexible. It must be generic enough to be employed in a wide range of situations, yet detailed enough to provide some degree of usefulness to a commander.

With all of these obstacles and challenges, trying to develop such a template is a formidable task. This section presents one possible template. By no means is this template meant to be the best possible such tool; rather, the hope is to provoke some thought about ways the template might be improved. Only by realizing the need for such a tool will constructive thoughts be put into action. The arguments presented here are not all-inclusive; as mentioned previously, no single discussion of IW could ever be. Thus, not all possibilities are considered. Again, the goal is to stimulate discussion on the subject. The ideas for the template are based largely on the author's own views, supported by a number of sources.[Refs. 32, 68, 88-90, etc.]

As a prelude to the ensuing discussion, an initial view of the template is provided in Table 11. Each entry will be discussed in at least some detail during the course of this section.

CATEGORY	SUBCATEGORY	COMPONENTS
Tangible	Politics	Domestic
		Foreign
	Economics	Commerce
		Finance
	Industry	Natural Resources
		Agriculture
		Manufactured Goods
	Essential Systems	Telecommunications
		Power Generation/Distribution
		Water Supplies and Sewage
		Heating/Cooling
		Transportation
		Space
	Geography	Physical
		Environment
	Military Forces	Personnel
		Doctrine
		Systems
Intangible	Culture	N/A
	Interests and Goals	N/A
	History	N/A

Table 11. Offensive Information Warfare Infrastructure Template.

This template is in the form of an "infrastructure". In this context, "infrastructure" is defined as

the collection of those items that can be used in constructing OIW target sets. The discussion of the template includes some of the things that comprise the particular subcategory or component, as well as some of the OIW tools and techniques that can be used for undermining that portion of the infrastructure. Some areas of this infrastructure template obviously lend themselves better to OIW than do others. As a result, some parts of the template will receive only the briefest of attention while others will be addressed at some length. One should also keep in mind that this template could also be used to some extent for waging more conventional forms of war. Finally, again, the discussion of this template is not meant to be all-inclusive, but, rather, to provoke further thought on the subject.

1. Tangible

The two major categories in the infrastructure template are Tangible and Intangible. Tangible is meant to be those things that can be easily seen or touched by OIW tools and techniques, either physically or pseudo-physically. Intangible is meant to be those things are that are not easily definable or touchable, yet can still be influenced by OIW (and often should be the primary focus). The Tangible category includes subcategories for: Politics, Economics, Industry, Essential Systems, Geography, and Military Forces.

a. Politics

The first subcategory is Politics. It consists of two main components: Domestic and Foreign. This subcategory is a logical starting point for a discussion of a country's infrastructure. This is the leadership of a country. It is perhaps the most critical node in the whole infrastructure. In the Warden model, leadership is in the center, and thus most important, ring. Great military thinkers throughout history (*e.g.*, Sun Tzu, Clausewitz, etc.) have

continuously addressed the importance of leadership, both political and military. A nation ultimately receives its orders to fight from its political leadership, not its military leadership (although they may be one and the same in some cases). Offensive Information Warfare can be used not only against a nation's foreign policy, but also against its domestic one.

Attacks against the political components are often the ultimate goal of an attacking force. Although direct attacks on the political arm are rare, almost every other subcategory of attacks discussed herein will influence politics in some way or another. These types of attacks, where the political branch is a primary strategic target from a tactical or operational attack on another subcategory, will not be addressed until the following section. There, the synergistic nature of the entire template will be considered in more detail. This subcategory is concerned mostly with ways to directly influence or target the politics of a nation.

(1) Foreign. The most obvious use of OIW in a political arena would be against an enemy's foreign policy. The intuitive goal is to influence that policy in favor of the friendly (*i.e.*, attacking) nation. For example, attacks against the foreign policy of an enemy could have the goal of swaying international opinion. A series of video-morphed and voice-synthesized newsclips, similar to those discussed in the previous chapter, could be used to mount a "smear" campaign to discredit the enemy in the international community. Other attacks could target critical supporting systems for that government. For example, a Denial of Service (DOS) attack could flood an enemy leader's computer networks at a time when such networks are critical. Other hacking or virus attacks could disable or degrade those same systems. These are but a few examples of the many possibilities.

(2) Domestic. Another way to influence the political sphere of an enemy is by targeting its domestic politics. The goal could be anything from destroying the "will of the people" (although this more aptly falls into the "Intangible" category discussed later in this chapter) to influencing local elections. In the first case, the same newsclips of atrocities mentioned could influence public domestic opinion against the *de facto* regime. If internal elections are largely automated in the second case, hacking attacks could be used to modify the results of an election to the point where candidates who are more amenable to the attacking force are elected. Again, the possibilities are endless. The ultimate goal in these types of attacks is to produce internal unrest. This unrest could range from annoying (such that the government is distracted from the international scene) to revolutionary (the people become so dissuaded that they want a radical change). Perhaps this latter scenario is a bit farfetched, but it is still definitely feasible.

b. Economics

The next subcategory is Economics, which has components of Business and Finance. Business is meant to include those organizations that deal in the buying and selling of goods. Finance in this context includes the monetary systems of a country (*e.g.*, banks, stock markets, etc.). The economics category is absolutely critical to any OIW campaign. The world in increasingly reliant on economic well-being in the international community. This, in turn, affects the domestic economic domain (and vice versa). Weak links in economic systems present definite COGs that could be exploited. As a result of the importance and complexity of the Economic subcategory in the world today, a somewhat detailed discussion of the process and possibilities is essential.

An outstanding publication from the Air University Press, entitled *Beyond The Industrial Web: Economic Synergies and Targeting Methodologies*, provides some insight into the diversity and complexity of modern economies, as well as a discussion of their importance. Although this work was written with the idea of exploiting conventional air power, many of the same ideas can be directly or indirectly tied to Information Warfare. The following discussion on some of these ideas presents many common themes and problems with any IW attack (*e.g.*, complexity of the systems involved, amount of knowledge required by the attacking force, etc.). Most of these ideas will be revisited either later in this chapter or in the following chapter.

A modern economic system is a complex one, and it is subject to Complexity Theory. Thus, all modern economic systems display several common characteristics derived from Complexity Theory. First, the various components of the system tend to interact with each other which causes the formation of a global behavior of the system (*i.e.*, the whole is greater than the sum of the parts). This global behavior is not totally predictable, regardless of the amount of detailed information that is available about the system. When looking at a complex economic system, one needs to look at the highest level (*i.e.*, the system as a whole rather than the individual parts). Second, complex systems tend to adapt to their environment, forming instinctive (but still complex) groupings. Third, complex systems become more complex over time, evolving "toward the edge of chaos"[Ref. 92] Finally, complex systems can process information. They can react to changes to their environment. The bottom line is that complex systems appear to be a living entity rather than a series of inert components.[Ref. 92]

From this explanation of modern economies as complex systems, one can see that targeting them is not trivial. Traditional analysis methodologies will not work against complex

systems. Indeed, a paradigm shift is needed. Only when such a shift takes place can effective targeting occur.[Ref. 98] Information Warfare is no different; a change in basic beliefs and thought processes is necessary before it can be fully exploited. Based on the fundamental change required in each case, Information Warfare appears to be the perfect weapon for targeting complex economic systems.

To reiterate a key point, economics is perhaps the most critical component in the world's structure today . Perhaps the best way to succinctly explain the rapid changes in the world economic community over the last twenty years is to present a quotation from an essay entitled "Economic Warfare: Targeting Financial Systems As Centers of Gravity" in which the author states:

> The late 1970s produced rapidly expanding and generally nondiscriminatory trade large-scale and rapid movement of funds from one financial center to another, and the rapid growth of multinational enterprises. Advances in transportation and communications technology have accelerated the interdependence. This economic interdependence has made national and international financial institutions critical to the smooth operations of nation-state economies. [Ref. 93]

This quotation not only shows the growth in importance of economics in the world order, it also shows its relationship to other critical systems, such as telecommunications and transportation. One should note also that those other systems are discussed as separate entries of this infrastructure template. Towards the end of the chapter, the discussion will focus on considerations for this template, including the relationship between template elements.

One widely-accepted measure of the economic power of any given country is its gross domestic product (GDP). GDP includes a conglomeration of five elements: banks, stock markets, foreign debt, value of exports, and value of imports. These five items are not directly

additive; rather, they have a linear regression relationship (*i.e.*, the interaction between elements must also be considered).[Ref. 93]

The goal of an OIW attack against an economic system should be to affect the GDP of the target country. Target sets would be drawn from the five GDP elements. However, one must also keep in mind the characteristics of complex economies. Only by maintaining a "system-high" perspective will effective attacks be possible. The five GDP elements could be also be further partitioned for easier understanding into a Commerce component and a Finance component.

(1) Commerce. Commerce is the practice of exchanging goods. Therefore, the exports and imports elements of GDP can be easily grouped together as a convenient target set. OIW attacks here could take the form of intrusive computer attacks (hacking) that result in changes to bills of lading, price fluctuations, changes in destination or quantity, or any number of other items.

For example, Country X routinely trades with Country Y. After covertly penetrating Country X's networked commerce system, Country Z manipulates it using OIW. This results in some of Country X's shipments to Country Y to be sent somewhere else. Of those goods that do arrive, they are of the wrong type or wrong quantity. After a period of time, Country Y gets tired of not getting what it paid for and finds another trading partner. Country X eventually traces the problem to "unexplained computer glitches". Of course, it is too late to convince Country Y of this fact. As a result, Country X loses a trading partner, their GDP suffers, and they lose status in the international community. Country Z has succeeded in

weakening Country X without firing a single shot and without Country X knowing about the attack.

(2) Finance. The other three elements of the GDP (banks, stock markets, and foreign debt) can be placed together to form a Finance component. Since most monetary transactions these days are performed electronically, the OIW potential in this area is great. Databases of transactions could be corrupted with a virus. Hacking attacks could change the prices of goods for unexplainable reasons, resulting in massive market fluctuations. Debt payments could be rerouted to a numbered Swiss bank account. DOS attacks could shut down entire portions of a stock market, resulting in large monetary losses. The end result is a decreased GDP in the target country.

Economic IW attacks are very powerful options in time of conflict. The results can be quickly devastating and far-reaching. Of course, these types of attacks could also trigger events in the world markets. Great care must be exercised to ensure an OIW attack does not inadvertently launch the world into an economic tailspin. Although these types of attacks are formidable, they are extremely difficult to accomplish, mainly due to the complexity of systems involved.

c. Industry

Another piece of the infrastructure template is Industry. This subcategory consists of three major components: Natural Resources, Agriculture, and Manufactured Goods. Attacks here can often be coupled with economic attacks to achieve the same common results (a decrease in GDP). Again, extreme caution must be exercised to avoid any unintended damage.

(1) Natural Resources. Natural Resources are vital to any country's survival. They form the starting point for manufactured goods that are either exported or used internally. If a country does not possess certain natural resources, then they are at the mercy of the international community to provide those resources. In an OIW campaign, propaganda attacks (in the form of specially prepared newspaper and magazine articles along with voice-synthesized radio broadcasts and video-morphed newsclips) could isolate a country from the rest of the world, thus denying them their required resources. Internal resources could also be affected. For example, oil pipelines that are computer-controlled could be shut down with a simple virus. One can easily see that something as unlikely as natural resources can also be an OIW target.

(2) Agriculture. Agriculture also presents potentials for OIW. Specific targets could be any number of specialized industries, from farmed goods to livestock. Perhaps the best example can be drawn from the recent "Mad Cow" disease scare in Great Britain. That country is taking steps, after almost being forced to by the European Union and world opinion, to slaughter over eleven million cattle. This will be a crippling blow to that livelihood. What if the whole thing were a farce, a deliberate attack launched by another country? Scientific studies could be forged. Samples are possibly tested by computers. That data can be changed to meet a given set of criteria. Coupling this whole process is a massive media campaign (the roots are planted and the "real" media takes over, accomplishing the attacking country's goals quite nicely). Again, the results could be devastating, and the victim country is never even aware that the whole thing has been fabricated.

(3) Manufactured Goods. Manufactured goods can also be influenced by OIW. Some of that was seen in the discussion of commerce above (goods could be rerouted). Other potentials also exist in this area. Studies for the demand of various products could be tampered with, resulting in either a glut or a shortage of certain products. Automated assembly lines could be shut down. For example, if the assembly line in a Chrysler assembly plant is shut down for more than twenty minutes, that entire shift of workers is sent home.[Ref. 94] This results not only in lost revenue for the plant and possibly a shortage of vehicles (which in turn could lead to higher prices of vehicles, etc.) but also in lost wages to the employees (who become disgruntled and go on strike, etc.). Imagine if all of that were to be accomplished by a carefully inserted Trojan Horse?

Industry presents a very lucrative target for OIW. Not many people think to protect these kinds of systems. Even if they do, probably not a lot of time and effort are spent on them. After all, the goal is to make money, and if there is no real threat (adopting the possible industry mentality for a moment), why spend the money on expensive protections? Besides, do not banks and stock markets make much better targets, with lots of money so easily available?

d. Essential Services Systems

Another very important subcategory in the template is Essential Systems. This subcategory is comprised of at least six major components: Telecommunications, Power Generation and Distribution, Water Supplies and Sewage, Heating and Cooling, Transportation, and Space. These Essential Services Systems are the things that most people think of when they think of a country's infrastructure (of course, this thesis has broadened that definition to include many more things). Since the first two components (Telecommunications and Power

Generation and Distribution) can possibly have a large impact on many of the other components in this template, each will be discussed in some detail in this chapter.

(1) Telecommunications. Telecommunications are an essential part of today's world. As one of the key aspects of the Third Wave revolution, telecommunications have become almost indispensable in almost facet of world society, to some degree or another. As a result, telecommunications systems should be considered as prime targets for employing Offensive Information Warfare.

Another outstanding treatise from the Air University Press, entitled *Taking Down Telecommunications*, provides great insight into the structure, vulnerabilities, and targeting methods for telecommunications systems. Although the work predates the most recent discussions of OIW (1994), it still stands as a masterpiece of Third Wave thinking (without the author even realizing that fact). This document serves as the inspiration for the somewhat lengthy (in comparison to other parts of this chapter) discussion of telecommunications that follows.

The importance of telecommunications, along with a brief discussion of some of the enabling technologies, was addressed in Chapter IV. To reiterate this importance, one can turn to the first page of *Taking Down Telecommunications*:

> It [telecommunications] permeates every face of society, thus allowing exploitation of information throughout the conflict spectrum at the tactical, operational, and strategic levels. Because of its data transfer capability and its mobility, telecommunications continues to increase in importance as a medium to direct our national instruments of power. Conversely, we must strive to deny the enemy the use of their telecommunications.[Ref. 95]

A structured methodology for "taking down telecommunications" is the goal in this portion of the chapter. Along the way, critical factors (*e.g.*, structure of systems, vulnerability analysis, etc.) will all be examined.

Prior to targeting any telecommunications system, a detailed working knowledge of that system, as well as its interaction with other systems and itself, is absolutely necessary. Like modern economic systems, modern telecommunications systems are extremely complex. As a result, the same ideas that were elaborated upon in the discussion of economic systems also apply here (*i.e.*, adaptiveness to environment, evolution toward chaos, etc.). Some of the workings of telecommunications systems were introduced in Chapter IV.

To further explore the intimacies of targeting telecommunications systems, Figure 10 (on the following page) presents a methodology for conducting vulnerability analysis. Although this diagram is almost a direct reprint from *Taking Down Telecommunications* (which really does not address Information Warfare *per se*), it is still an outstanding tool for preparing OIW target sets against telecommunications. By the end of the deliberation about this diagram, the reader should be familiar with the multitude of factors involved in targeting telecommunications systems.

The Telecommunications Vulnerability Assessment Methodology shown in Figure 10 can be broken down into basically three parts: systems analysis (shown on the y-axis by the entries under the boldfaced and underlined "Physical Categories" and "OSI Layers"), "Perspectives" (shown by the entries on the x-axis at the top of the diagram), and "Vulnerability Questions" (shown by the entries along the z-axis of the diagram). Each part is discussed in further detail below.

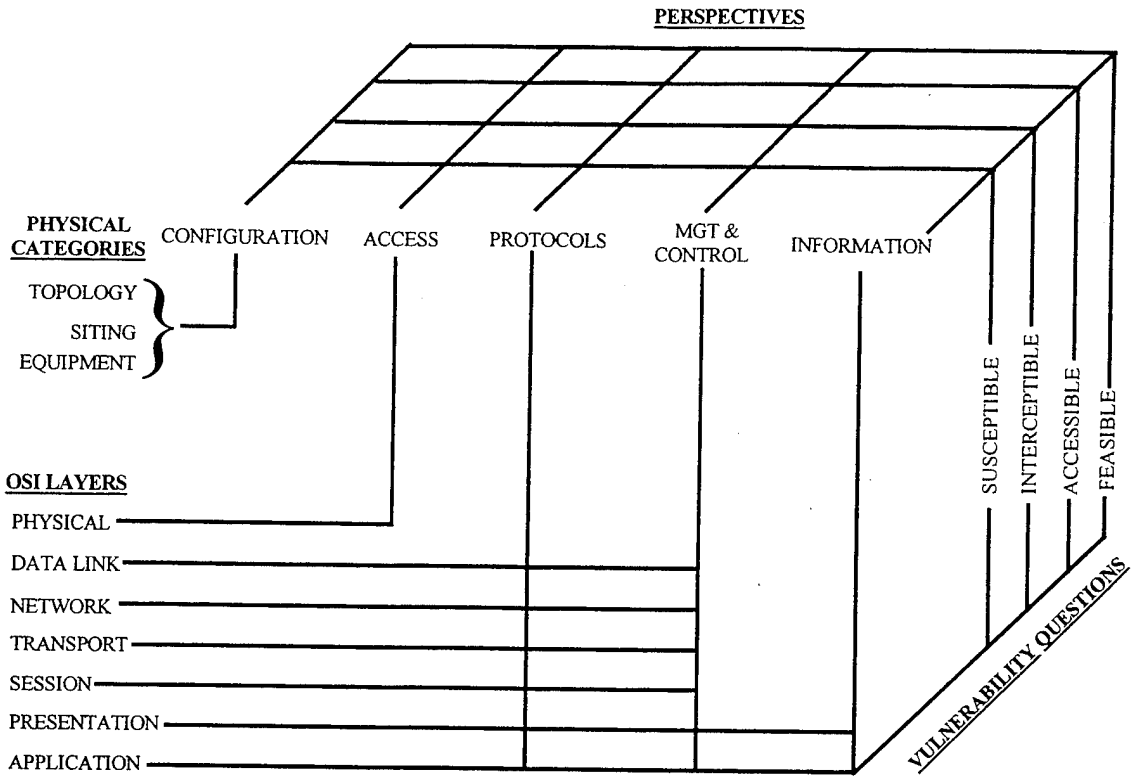

Figure 10. Telecommunications Vulnerability Assessment Model.[From Ref. 95]

The systems analysis portion consists of two parts: Physical Categories and OSI Layers. The Open Systems Interconnection (OSI) Model is a set of seven layers, each of which performs separate functions. Together, they form the total system. The OSI Model is an increasingly popular way to analyze and construct computer systems. Since the majority of modern telecommunications systems are now computerized, this model is very appropriate to their study.

The seven layers are shown below [Ref. 95], along with a brief description of each :

- Physical Layer -- This is the most basic level. It is essentially the hardware requirements (*i.e.*, voltages, pin numbers, etc.) for information transfer.[Ref. 95]

- Data Link Layer -- "This layer regulates the flow of information bits."[Ref. 95]
- Network Layer -- The algorithms that control the transportation of packets of data reside in this layer. This layer also knows the layout of the network.[Ref. 95]
- Transport Layer -- This layer is responsible for establishing and maintaining connections between users of a network, even those using dissimilar systems.[Ref. 95]
- Session Layer -- Synchronization of users is the purpose of this layer. Here is where the controlling algorithms for user connections are held.[Ref. 95]
- Presentation Layer -- This is the syntax layer. This is where different types of computer languages can interface. Encryption can also occur in this layer.[Ref. 95]
- Application Layer -- This is the layer where the user interfaces with the computer. Algorithms are system-specific here, providing information to the user in a recognizable form.[Ref. 95]

A distinction between the first six layers and the final layer can be made. The first six layers contain the protocols for the system; exploitation of those layers can affect other systems. The Application Layer is user-specific; it can be used for directed attacks (against a particular user or a particular terminal). On the other hand, a virus that is introduced at the Network Layer could possibly affect any other system on the network. This may or may not be the purpose of a given attack. Thus, one can easily see that an in-depth knowledge of an enemy's networks is necessary, as well as a plan that covers all possible contingencies, prior to commencing OIW hostilities.[Ref. 95]

The other half of the systems analysis group, shown under the heading "Physical Categories", are the three actual physical characteristics of the system in question. First, Topology denotes the actual physical layout of the telecommuncations network. Next, Siting is the physical location of all components and supporting facilities of the network. Finally,

Equipment deals with the physical properties of the equipment used by the network components (*i.e*, transmission media, modulation scheme, etc.). An examination of the physical categories of a telecommunications system is necessary to determine common threads and vulnerabilities as well as matching of OIW tools and techniques.[Ref. 95] For example, an EMP bomb might be more effective against a telecommuncations system that relies heavily on microwave towers than against one that is almost exclusively connected by underground fiber-optics cables. In another case, if the enemy has the majority of the primary and backup system components in plain view, physical destruction might be the preferred attack method (*i.e.*, area bombing).[Ref. 95]

The next major part of the Telecommuncations Vulnerability Assessment Model is "Perspectives" (again shown along the x-axis at the top of Figure 10). This portion consists of five factors. They are listed below, along with almost a verbatim description from *Taking Down Telecommunications*:

- Configuration -- This perspective concerns itself with the "physical properties of the network".[Ref 95]
- Access -- Here one is looking at "susceptibility to enemy access into the system".[Ref. 95]
- Protocols -- The question of interest here is "once access is gained, how susceptible are the system's data transfer service, routing, flow control, etc."?[Ref. 95]
- Management & Control -- This perspective deals with "information concerning network ability to adapt to congestion, adaptive routing, etc.".[Ref. 95]
- Information -- Here the focus is "mission-related information actually reviewed by a user/decision maker".[Ref. 95]

Appendix A of *Taking Down Telecommunications* contains lists of over 140 specific questions that address these perspectives. This is an excellent source of information, and the reader is

referred to it for an in-depth look at the kind and detail of knowledge that is required to target a telecommunications network. These kinds of attacks are far from trivial.

Now one can combine the x and y axes of Figure 10 to see where each affects the other. For example, the Presentation Layer and the Application Layer are concerned with all five of the Perspectives discussed above. On the other hand, the entire "Physical Categories" portion of the systems analysis axis is only affected by the Configuration Perspective (which fits what one would expect). One will also notice that six of the seven OSI Model Layers are influenced by at least four of the five perspectives. The relationships between these two axes are extremely complex and detailed. The reader is again referred to Appendix A of *Taking Down Telecommunications* for some of the specific information items required.

The final piece of this methodology is the z-axis, which contains four "Vulnerability Questions". These questions can be most easily explained by a direct quotation:

> First, how *susceptible* is a system architecture to interference. Second, to what extent can one *intercept* network information flow describing how the system works thereby gain[ing] the knowledge necessary to disrupt the network. Third, is it possible to gain *access* to the network to interfere with its functions. Fourth, is it *feasible* to attack the system (*e.g.*, do the objectives of attacking or penetrating the system, or parts of it, justify dedicating the resources required to obtain those objectives).[Ref. 95]

One must answer all four of these questions for <u>every</u> entry in the x and y matrix. Only if satisfactory answers for <u>all four</u> questions can be obtained can the telecommunications network be assumed to be vulnerable to an OIW attack. If satisfactory answers cannot be obtained in each case, the chances of success are probably not very high.[Ref. 95]

The discussion presented here for using OIW attacks against modern telecommunications systems has centered around a structured methodology. This detailed

methodology focused on a vulnerability assessment of a telecommunications system. Once this highly complex assessment is complete, only then can the right kind of attack be planned and executed. Once the scope is set, the right mix of OIW tools and techniques can be applied to obtain the desired goals.

(2) Power Generation and Distribution. Another extremely critical component of the infrastructure template is electric Power Generation and Distribution. Electricity is indispensable in the modern world. Almost every system discussed in this chapter, especially computer systems, rely heavily on electricity to function. Although advances are being made in other power generation media (*e.g.*, batteries and others as discussed in Chapter IV), the majority of the industrialized world depends on electric power for survival. As a result, such power generation and distribution systems should be considered as vital targets for OIW attacks.

For example, electric power systems could (and most likely are for the majority of countries today) critical COGs in all five rings of the Warden Theory (see Figure 8 and accompanying discussion). If electricity were lost, the innermost ring (Leadership) would be severely degraded. Communication and guidance would be severely handicapped. Of course, there should be backup systems, but these will most likely lack the power and sustainment of the primary systems. In the second ring (Organic Essentials), loss of electricity would mean loss of systems that supply water, refrigeration, industry, and many others. If the loss were to extend to the third ring (Infrastructure), then such things as transportation sytems become affected. Loss of electricity to the fourth ring (Population) means a loss of power to the homes of the civilian population (which can have a very powerful effect on the Leadership ring, if protracted). Finally,

electricity could be lost to the last ring (Fielded Forces). Naturally, the effect to this ring would probably be felt the least (because of backup and mobile systems), but there would most likely be some reliance on traditional forms of electric power (*e.g.*, mainframe computer systems).[Ref. 96] One can easily see the heavy reliance on electricity in all facets of society.

The complexity of modern electric generation and distribution systems demands a vulnerability analysis methodology, similar to the one discussed under the Telecommunications component. Luckily, the frugal origins of one already exist. In late 1994, Air University Press released what proved to be a very controversial (because it was cleared for public release) work entitled *Electric Power Simulation (EPS) Concept Prototype: Dropping The Electric Grid, An Option For The Military Planner*.[Ref. 96] This publication and its accompanying software tool are an excellent method for examining electric systems. Both the book and the program are full of detailed information about electric systems. Although the prototype lacks much of the functionality promised in the full production version, it still represents an excellent starting point for any study into using OIW against electric systems. Even though the publication was written primarily for using conventional destructive weapons, much of the same thought processes can be applied to IW. As a result, this discussion of Power Generation and Distribution will rely heavily on this work as an example of the type of procedures that must be in place to effectively wage OIW in the electric realm.

In the EPS text, a four step methodology is discussed. The steps are listed below and each is expounded upon in the subsequent paragraphs:

- Step 1. Component Structure.
- Step 2. System Structure.

- Step 3. Criticalities and COGs.
- Step 4. Vulnerabilities.

This methodology will serve as the basis for the examination of the Power Generation and Distribution component of this template. One should bear in mind that this methodology is non-linear. Also, the explanation of the methodology will focus on thermal generation systems. Although other forms do exist (*e.g.*, nuclear, hydroelectric, etc.), time and space do not permit a detailed discussion of each type. Furthermore, the preferred fuel for most thermal plants in the world today is coal (by a factor of three to one).[Ref. 96]

The first step in the methodology is Component Structure. Here one is looking at the physical equipment of the system in question. Obviously, some knowledge of what comprises a given system is necessary before targeting it. Although different power generation plants are configured differently, they all have almost the same nine subsystems. Those nine subsystems are listed below, along with a brief description of each:

- Generation -- Basically, in this step, the kinetic energy of the working fluid is converted into rotational mechanical energy.[Ref. 96] This rotating mechanical energy is introduced into a magnetic field which generates electricity.
- Step-up Transformer -- Transformers (essentially just a series of windings for changing voltage values) are used to convert the relatively low voltages produced by the generators into higher voltages that are acceptable for transmission.[Ref. 96]
- Transmission -- The electricity is then moved through conductors, insulators, supports, and shield wires. These are the power lines and structures that are seen everywhere. Above-ground transmission is generally preferred to the more secure underground transmission because the latter brings with it a tenfold cost increase.[Ref. 96]

- Switching Stations -- Switching stations are used to partition the electric power network into manageable chunks in order to assist troubleshooting of problems.[Ref. 96]

- Primary Substations -- These facilities are used to step-down the voltage from the higher transmission values into those that are more manageable for further distribution. These sites are generally unmanned and automated.[Ref. 96]

- Subtransmission -- This step is essentially the same as the transmission function discussed above.[Ref. 96]

- Distribution Substations -- These substations are similar to the Primary Substations except they are located closer to the customer and control less area. They are also unmanned.[Ref. 96]

- Primary Distribution -- At this point, the final step-down in voltage occurs and the electricity is distributed to the customer. This distribution generally occurs at a pole-mounted transformer adjacent to the customer's location.[Ref. 96]

- Secondary Networks -- This final subsystem is generally found only in areas of high electricity demand. They are used to more efficiently distribute the power.[Ref. 96]

Of course, interspersed throughout all of these subsystems are protective features, controls, overrides, alarms, etc. Even though more and more of these features are becoming automated, there will probably always be some form of manual switching and control in most systems.

The second step in the EPS methodology is System Structure. In this step, one is looking at the entire power distribution system of a target country. At this level, one can easily see that the system of any modern country will be highly complex. As a result, the same approach to complex systems that was discussed under the Telecommunications component must also be applied here. The interaction between subsystems must be considered. A complex power generation and distribution system will appear to take on a life of its own (in keeping with the characteristics of a complex system).[Ref. 96] Naturally, an analytical approach similar to Figure

10 in the Telecommunications explanation is needed. Luckily, thought has already started in this area (in the form of the EPS software, which will be discussed later).

The third step is Criticalities and COGs. Here, the goal is to identify what subsytems and locations are critical to the entire systems, such that their exploitation will cause serious damage to the enemy and meet the required objectives. These critical links then become COGs. Many factors must be considered in making these decisions. Some of these include: time to repair, cost to repair, extent of impact, etc.[Ref. 96]

The final step in the EPS methodology is Vulnerabilities. Now that the system has been analyzed and COGs identified, the next logical step is looking for weaknesses in those COGS. In its discussion of this phase, the EPS book falls short and does not provide many specifics for accomplishing this. Perhaps this is due to the enormous scope that such an explanation would entail. One solution is the creation of a vulnerability assessment matrix, similar to the one used previously in the discussion of telecommunications.

Included with the EPS text is a prototype software tool. It is designed primarily for analysis of electric grids. Related systems (such as telecommuncations, culture centers, water, etc.) are also considered in the analysis. The system is quite user-friendly; in fact, if the user tries to perform an attack that is not on an optimal COG, the program informs the user of that fact. Additionally, the system contains a wealth of information, complete with pictures and diagrams, about the details of the various types of power generation systems that exist (*e.g*, nuclear, hydroelectric, etc.). Although this system was designed with conventional air power as the delivery platform, the transition to an exclusively OIW system is feasible. Unfortunately,

such a system would require an extensive and detailed database of the system in question (this problem will be revisited in the next chapter).

With this entire methodology in mind, what portions of a power generation and distribution system should be exploited using OIW tools and techniques? Of course, there is no single answer. The most obvious targets might be control centers. Here, hacking attacks can occur and malicious software can be injected. Of course, physical destruction is another realistic option (although these types of attacks border more on traditional forms of warfare than IW). Other methods could also be used. Air-dropped microbes would do wonders for consuming exposed electrical components. Well-placed EMP bombs could quickly drop portions of the electric grid.

One needs to keep in mind that in order for these things to be OIW attacks, they must be focused on epistemological targets. For example, the dropping of an electric power grid could coincide with the launching of a Psychological Operations (PSYOPS) campaign. This campaign could be directed at the general populous to undermine their will and support for their leadership. If the electricity is down, the enemy leadership would be hard pressed to refute any false information that is broadcast by attacking forces. This is but one scenario out of many that could be used in conjunction with attacks against power generation and distribution systems.

(3) Water Supplies and Sewage. The next major component under Essential Services Systems is Water Supplies and Sewage. These types of systems are absolutely vital to the survival of any nation or group of people. As a result, they could be targets for OIW attacks (most likely indirectly). Perhaps the most effective technique would be making the enemy and its people believe that its water supply is contaminated. An extensive PSYOPS

campaign could be used to accomplish this goal. The impact of such an epistemological attack could be enormous; without drinkable water, the enemy may be forced to capitulate. After hostilities, friendly occupying forces make motions of restoring the water supply (with an "antidote" for example) while in reality nothing is changed because the water is not really bad. The end result is achievement of friendly objectives with minimal losses, and the enemy is none the wiser on how it was accomplished.

(4) Heating/Cooling. Heating and Cooling Systems are commodities that are taken for granted in large parts of the world today. Many people assume that a prolonged loss of those services would be merely an inconvenience. Would they still be saying the same thing if they lived in a very cold climate and all of their natural gas supply were to disappear in the middle of a harsh winter? By taking over the computers that control the routing of natural gas, this scenario is possible. Perhaps a better way would be the corruption of a database in a natural gas provider's computers. "We're sorry, Customer A, we would really like to provide our service to you, but our records show that you have not paid your bill in four months. Have a nice day." If this were to be accomplished on a large scale, chaos could ensue. This is but one example of using OIW against Heating and Cooling Systems.

(5) Transportation. Any society, and especially an industrialized one, relies heavily on transportation. People and goods can be moved from one corner of the earth to another fairly quickly. Most people take this service for granted. A series of OIW attacks might make them think again. What would happen if the air traffic control networks for an entire country (a large, industrialized one) were to cease functioning over a holiday weekend? At the same time, all of the drawbridges in the capital city become stuck in open position because of

"computer problems".[Ref. 70] To make matters worse, all of the traffic light controls for that city also go down. While all of this happening, friendly forces launch an assault on the capital city, taking advantage of the chaos to quickly seize control. As this scenario shows, OIW can be a very welcome addition to a warfighter's tool chest.

(6) Space. One area that is often overlooked when thinking of Information Warfare, and the final component under Essential Services Systems, is Space. The increasing reliance of many countries on timely communications systems has seen a commensurate increase in the number of space-based systems. Some of those systems, as well as some their vulnerabilities, were discussed in Chapter IV. In an OIW PSYOPS campaign, a necessary first step might be gaining access to a communications satellite channel (while jamming other channels and satellites). Space can be an OIW force multiplier.

e. Geography

The next major subcategory where OIW can be exploited is Geography. This subcategory can be further defined by the components Physical and Environment. One may think that geography would not even be considered in OIW planning. Although the possibilities are limited, some do exist.

(1) Physical. The Physical aspect of this template is more of a consideration for OIW than a targetable area. Geography can influence the planning for an OIW campaign. The type of terrain involved, the size of the area in question, geographic limitations to both friendly and enemy forces [Ref. 93] are all things that must be looked at in planning OIW attacks. Based on such an analysis, different types of OIW tools or techniques might be preferable or prohibitive. For example, a communications outpost that is located high on a

remote cliff might not be an optimal target for a HERF gun or a Van Eck detector. In any case, the physical features of a country are factors which should be addressed.

(2) Environment. A related component is the Environment. The world is becoming more and more environmentally conscious. As a result, people do not like to see damage done to the environment. A carefully orchestrated PSYOPS plan could create false pretenses in a target country that environmental damage is being done by their own government. This, in turn, could create dissatisfaction, undermine the will of the people, etc. Also, the environment must be considered when planning an OIW campaign. By sending other systems (*e.g.*, electric, industry, etc.) that have direct ties into the environment (*e.g.*, emergency waste dumps into rivers, etc.) into chaos, the possibility exists for real environmental disaster. Of course, this is probably not something a reasonable country would want to do.

f. Military Forces

The final item to consider on the Tangible side of the infrastructure template is Military Forces. Military Forces make an obvious target for any type of warfare, including Information Warfare. The Military Forces subcategory discussed here is directly related to the Fielded Forces ring in the Warden Five Rings Theory mentioned previously. Thus, it is a critical COG of an enemy and should be targeted. The three components of the Military Forces subcategory are: Personnel, Doctrine, and Systems.

(1) Personnel. The people that comprise the Military Forces of the enemy are OIW targets. The most obvious OIW technique against humans is PSYOPS. Several examples of these kinds of attacks have been mentioned in this chapter and the previous one. The goal here would be deceive the enemy's military personnel to the point where they would

lose faith in their leadership and not want to fight anymore. This, obviously, would give friendly forces a tremendous advantage. Even if they do not surrender or run away, an effective PSYOPS campaign could plant seeds of doubt in the minds of the enemy soldiers that make them hesitate at a critical moment.

(2) Doctrine. The second component that could be attacked under the Military Forces subcategory is Doctrine. This component could almost be considered as an intangible element of this template. However, if one considers the doctrine as just the actual methodology for warfighting and ignores the underlying beliefs for it, then this is the right place for doctrine. Using OIW against a country's beliefs will be examined in the Intangible portion of the template. By gaining insight into military doctrine, attacking forces could derive operational and tactical COGs that could be exploited. For example, if a review of doctrine reveals that in a given situation, enemy forces will always react a certain way, this fact could be manipulated using OIW tools and techniques to achieve a desired goal.

(3) Systems. The final, and most obvious, component of the Military Forces subcategory is Systems. Any military force is going to rely on a given set of systems to support their operations. Many of these will parallel civilian systems or even tie into them directly. Examples of military systems include such things as telecommunications and power generation and distribution. There are essentially two levels of systems here: those that tie directly into civilian systems (*e.g.*, Internet access or phone lines to a commercial telephone company) or those that are exclusively military systems (*e.g.*, portable power generation systems or military telecommunications systems). OIW attacks against the former are fairly straightforward and are discussed elsewhere in this chapter. Attacks against the latter may

require more skill and effort, as well as possibly different tools and techniques. In any case, OIW attacks against all three components of the Military Forces subcategory should be considered as a vital part to any OIW plan.

2. Intangible

The second major category for this OIW template is Intangible. This category consists of those things that are not necessarily directly attackable by OIW tools and techniques, yet can be influenced by them. Using OIW against these Intangible elements is no easy task. There are no measurable quantities to execute. Different perspectives on the same subject may yield different results. However, these Intangible factors must be addressed in OIW; they serve as the primary basis for most of the epistemological target sets discusses previously. Only with a thorough understanding of the items presented here can one translate that knowledge into tangible target sets.

a. Culture

Many experts in warfare will say that in order to effectively wage war against an enemy, one must know how they think and why they act the way they do in certain situations. A large part of this revolves around the first subcategory of the Intangible category, Culture. A good inroad into understanding a given culture is learning the language; language is closely tied to culture. Of course, the language of every possible adversary can not be learned by everyone who needs to know it (major decision makers, detail planners, tactical commanders, etc.). Computers can help in this regard (*e.g.*, artificial intelligence, neural networks, interactive databases, etc.), but they can never replace the subtleties that the human element can garner. By

understanding the culture of a country, OIW attacks can be targeted against weak links in beliefs and perceptions.

b. Interests and Goals

Once a thorough understanding of an enemy's culture is gained, the task of discerning what their Interests and Goals are becomes much easier. Many times, the things that a country desires can be understood from a thorough knowledge of their culture. Getting inside the enemy's mind to uncover his or her agenda is the first step in leveraging a successful OIW attack. A truly masterful OIW attack would be one that is able to attack those goals and interests directly, perhaps even changing them somewhat without the enemy even knowing.

c. History

A final Intangible component is History. The study of history can often uncover many things that can be used to an attacker's advantage. For example, in previous conflicts, what were the COGs that were used successfully against that enemy? Do such weaknesses still exist and can they be exploited this time? History can also be used to look at trends in government, how or if a country binds together during a war, etc.[Ref. 93] Although there is not much (if any) history relating to an Information War, many of the same vulnerabilities could be manipulated, albeit in a different fashion.

The construction of the template is now complete. Again, this template is not meant to be a perfect solution or an all-encompassing one. It should be used as a general set of guidelines of things to be examined when putting together an Offensive Information Warfare campaign plan. Obviously, most of the entries in the template have several tools and techniques that could be used with them. Only a few brief examples were explored here, for brevity's sake. One might

notice that some things have been omitted from the template. For example, OIW attacks against hospitals might be a very powerful weapon (*e.g.*, scrambling medical records or changing diagnoses). However, such things might be counterproductive. Plus, many safeguards (*i.e.*, international law) are already in place for such things. To summarize the infrastructure template first shown in Table 11, is reprinted on the following page as Table 12. The end result of this section is that template. If used properly, it should be consistent, flexible, and generic while remaining useful. Of course, it is not a perfect template, and changes to it could (and should) be made as required for improvement.

C. REVIEWING THE INFRASTRUCTURE TEMPLATE

After examining the infrastructure template, at least four recurring themes come to mind. All of these have been mentioned at least once during the template construction. They are elaborated on here from an overall perspective. The four items are: Interaction of Template Elements, Complexity, Restoration and Redundancy, and Measures of Effectiveness.

1. Interaction of Template Elements

The infrastructure template is not one of isolated entries. Rather, there is an interaction between template elements. Some of these interactions may be stronger than others. Some may be planned, others may not. The end result is a synergistic effect throughout the template. Indeed, true success in an OIW campaign is a result of recognizing and maximizing this synergistic effect. Failure to consider this interaction can result in defeat (*i.e.*, by not realizing that attacking one element in the template could possibly adversely affect another element).

CATEGORY	SUBCATEGORY	COMPONENTS
Tangible	Politics	Domestic
		Foreign
	Economics	Commerce
		Finance
	Industry	Natural Resources
		Agriculture
		Manufactured Goods
	Essential Services Systems	Telecommunications
		Power Generation/Distribution
		Water Supplies and Sewage
		Heating/Cooling
		Transportation
		Space
	Geography	Physical
		Environment
	Military Forces	Personnel
		Doctrine
		Systems
Intangible	Culture	N/A
	Interests and Goals	N/A
	History	N/A

Table 12. Offensive Information Warfare Infrastructure Template.

2. Complexity

Much has been said about the nature of complex systems, especially in dealing with the template components of Telecommunications and Power Generation and Distribution. However, complexity is practically inherent in any modern system. Although not specifically mentioned under other components, one should assume that such complexity does exist. As a case in point, there was no mention of complexity in the Transportation component (mainly due to a lack of documented examples); however, one merely needs to look at any network diagram of a modern traffic control system to see such complexity. Two very powerful methods for dealing with complexity were mentioned in this chapter. The first was the vulnerability assessment methodology shown in Figure 10. The second was the EPS simulation software mentioned in the Power Generation and Distribution component. These represent preliminary steps that need to be refined. Systems will continue to grow more and more complex. Preparations need to be made to deal with those kinds of systems (perhaps using such technologies as neural networks). A study of Complexity Theory should be a basic tenet in any course of study about Information Warfare.

3. Restoration and Redundancy

A third theme is Restoration and Redundancy. Any well-built system is going to have an inherent redundancy capability, a quick restoration capability, or both. This must be considered when planning OIW attacks. Neutralization of one or more system elements may not have the desired overall effect. A thorough understanding of the restoration and redundancy features of a given system is necessary. Effective use of probing and mapping tools can facilitate this. One should also keep in mind that perhaps full effectiveness cannot be achieved in this arena. As

systems become more complex, they evolve toward the edge of chaos; in other words, affecting one element of a system may have a totally unpredictable effect on the system as a whole.

4. Measure of Effectiveness

One of the most difficult problems in using Offensive Information Warfare in a campaign setting against an infrastructure is assessing the effectiveness of the attacks. Measures of Effectiveness (MOEs) are a challenge and a necessity to modern warfighting. Since Information Warfare is a relatively new discipline, there are really no "tried and true" MOEs. In fact, the rapid proliferation of systems and technologies may prohibit such MOEs from evolving.

The solution lies in a paradigm shift about the way MOEs are viewed. Many people may be reluctant to try "new" MOEs that are not well-understood. Perhaps existing MOEs could be used if they are viewed in a lightly different manner. For examples of existing MOEs, *Taking Down Telecommunications* provides five MOEs for evaluating attacks against those types of systems. They are listed below, along with a brief description of each:

- Grade of Service (GOS) -- This MOE is used to determine the "loss of system capability in a static system".[Ref. 95] It is calculated by dividing the amount of network traffic available after the attack by the amount available before the attack. Obviously, a lower number means the attack was more effective.

- Range -- This MOE is simply the range at which information can be heard.[Ref. 95] This is useful, for example, in jamming attacks.

- Throughput and Delay -- Throughput is a measure of successful data transmissions per unit time. Delay is the amount of time between transmission and reception of a given message.[Ref. 95]

- Utilization -- This MOE is a measure of how much a given system is in use, compared to its maximum loaded state.[Ref. 95]

- Availability -- This final MOE takes into consideration such things as reliability (accurately providing information to the intended user) and survivability (how well the system is able to function after a given attack).[Ref. 95]

Most of these MOEs might be a good measure for many OIW attacks if the goal is to degrade the given system. However, how does one accurately measure the number of programs that have been infected by a virus? The system may not be degraded from a GOS standpoint, but it is definitely being degraded if the virus is propagating throughout the enemy's networks. One can easily see new MOEs are definitely needed. However, developing them will be no easy task.

This chapter has presented a planning tool for the employment of Offensive Information Warfare. It started with a somewhat detailed review of Centers of Gravity. Included therein was the Warden Five Ring Theory. The need for a tool such as an infrastructure template was then examined, including a look at the Information Warfare Battlespace and a review of the Offensive Information Warfare Strategy. The majority of the chapter was spent developing the infrastructure template. Of course, this template is not perfect. It is only meant to provide an entry point into effective OIW planning. The examples provided were basic and were only a small sample of many possibilities in this field. During the construction of the template, several recurring features were noted. They formulated the basis for the final section of this chapter. With the template clearly defined, the next logical step is to examine why or why not one might want to use Offensive Information Warfare.

VII. OFFENSIVE INFORMATION WARFARE ISSUES

A. THE DECISION TO USE OFFENSIVE INFORMATION WARFARE

The decision of whether or not to use Offensive Information Warfare is not a trivial one. As one can now see, the weapons, technologies, and targeting criteria are all very complicated. In addition to all of the things that go into constructing an attack, other consideration must be given to a wide variety of issues. These issues are extremely important and they cannot be ignored. This chapter discusses some, but perhaps not all, of those types of issues. These explanations center around two major groupings: "Major Issues" and "Other Issues and Considerations". The former category deals with topics that are absolutely critical to a decision of whether or not to use Offensive Information Warfare. The latter category is more concerned with things that must be taken into account once the larger issues have been resolved. They are more focused toward the execution of OIW rather than towards the decision to employ it.

If the author of this thesis has been successful, the reader will, it is hoped, have realized by now that Information Warfare is definitely warfare and it should definitely be employed by the United States if possible (the last part of the OIW puzzle is this chapter). In many cases, OIW is a totally new way of thinking (*i.e.*, a paradigm shift). Those who are not willing to make the shift will never understand until they become victims of OIW. Information Warfare can be very powerful yet very complicated. This chapter looks at some of the hard questions associated specifically with Offensive Information Warfare. Of course, the arguments presented here are not meant to be the only possibilities; rather, they are meant to provoke further thought and to show how tough some of these problems can be for potential decision makers. Other than the

multitude of definitions' arguments (explored in Chapter II) , some of the items discussed in this chapter are among the most controversial in Information Warfare circles today.

The world order and the domestic community of the United States are very complicated (they could, in fact, themselves be considered as complex systems). As a result, decision makers in the United States must be very tuned to a large number of sensitivities and expectations from both the national and international communities when contemplating any kind of military option. Some of those considerations (herein after referred to as "the bulleted list") include:

- U.S. forces should have the ability to act quickly and decisively, with minimal (preferably zero) casualties and with minimal impact on the environment.[Ref. 97]
- The U.S. should be able act in situations of less than total war and be able to avoid long, drawn-out conflicts (the Vietnam syndrome).[Ref. 97]
- U.S. forces should be able to operate effectively (*i.e.*, with a high degree of precision) in a complex arena interspersed with both combatants and non-combatants.[Ref. 97]
- The U.S. should be able to use its strong military prowess to avoid conflict whenever possible. If military force is necessary, there will be clearly defined goals, missions, and a time line for completion.[Ref. 97]
- All of these things should be accomplished while maintaining the "moral high ground" and while under "constant media scrutiny".[Ref. 97]

These questions are always in the minds of the leadership of the U.S. when trying to make a decision about using military force. These same points will serve as critical points for many of the issues discussed in this chapter. While other sensitivities do exist, the ones presented here are among the most important. As a result, the bulleted list will be referred to throughout this chapter.

B. MAJOR ISSUES

The first grouping of OIW issues and considerations are Major Issues. This category includes four subcategories: Political, Legal, Economic, and Moral and Ethical. These are the toughest issues that face any of the major decision makers (President, military commanders, etc.) when trying to determine whether or not to use OIW in a given situation and to what extent it should be used. The wrong decision in any of these subcategories could have disastrous results, most notably on the United States. Perhaps others that could be affected by a poor decision include allies and civilians. Therefore, great care must be taken when tackling these tougher issues (tougher when compared to the issues in the next section; both categories are difficult, but this one is more so, perhaps).

1. Political

Since any form of conflict revolves around the political scene, the first consideration to address when contemplating OIW attacks is the Political subcategory. The decision to implement any OIW campaign plan is going to come ultimately from the National Command Authority (NCA), comprised of the President of the United States and the Secretary of Defense. Before giving assent, they will want to ensure that all (or as many as possible, given tradeoffs) of the international and national considerations (as listed above) will be assured by this plan. In many cases, OIW can satisfy most of those requirements. OIW attacks can be swift and decisive if properly prepared (as discussed in the following section), and they can operate in extremely complex situations. They can be accomplished with little or no loss of life. Certain attacks can be targeted against combatants only, excluding non-combatants. The nature of OIW demands that they have clearly defined missions, goals, and time lines.

Of course, there are potential negatives with OIW as well. OIW attacks can be covert; this may be bad if the U.S. is seen to do nothing in the eyes of the world community. In the harshest forms of OIW, civilian populaces can be affected dramatically, both subtly and devastatingly. Some tough decisions will have to be made as to whether the objectives of the campaign require such actions. If the answer is yes, there exists the real possibility of the media doing damage and of the U.S. losing the "moral high ground".[Ref. 97] Other drawbacks could be inadvertent effects on allied nations *(e.g.*, a PSYOPS campaign could just as easily affect friends as enemies, a fact not likely to be appreciated if the former were ever to find out).[Ref. 98] The bottom line is that public opinions and perceptions are likely to be heavy factors that will influence any political decision on whether or not to use OIW.[Ref. 99]

2. Legal

Another very complicated and hotly debated issue surrounding Offensive Information Warfare is its legality. To date, no formal laws have been enacted, either in the United States or in the international law arena, that specifically address this evolving warfighting discipline. As a result, one can only look at existing statutes and see if they can be interpreted to either encourage or discourage OIW attacks. Obviously, the United States would never want to do something that could be construed as illegal...at least if there were a chance of anyone finding out. There may, however, exist a situation where skirting the edge of the law might be preferable to the consequences of taking no action. Again, this is another tough decision for the political element. The plethora of legal debates can be grouped into two convenient categories. They are Domestic and International. The former refers to laws particular to the United States while the latter is concerned with laws in the international community. These legal squabbles over existing laws

are not likely to be much affected by the considerations shown in the bulleted list above, but the leadership still needs to be able to justify their decisions to their people and to the world.

a. Domestic

There are many documents within the United States legal system that could form the basis of decision about the legality of Offensive Information Warfare (*i.e.*, a justification for OIW). These include: the Constitution, parts of the United States Code, various Congressional acts, and various Executive Orders. Of course, there could be many other statutes that could be interpreted as a pro or a con for OIW. For the purpose of this thesis, a few samples from the above categories will be discussed with respect to their possible effect on OIW. Noticeably absent will be an examination of statutes pertaining to OIW-type attacks directed against the United States; those laws fall more aptly into the Defensive IW sphere.

As mentioned above, possible interpretations for OIW can be gleaned from a variety of legal sources. The Constitution of the United States could possibly be considered. Examples are the clauses that state the powers to "declare War" or "make all Laws which shall be necessary...".[Ref. 29] If IW is a form of warfare, then the former applies. The latter phrase could be a very loose catch-all (the "if nothing else works, try this " mentality) to justify an OIW attack.

The United States Code could also be used for OIW justification. Title 10[Ref. 100] deals with Armed Forces and is often quoted ("Organize, Train, and Equip") as a justification for IW in general. Section 164[Ref. 100] outlines the powers and duties of the combatant commanders (CINCs). Included therein are powers to organize and employ forces. Section 121[Ref. 100] says that the President (in his capacity as Commander-in-Chief) may

"prescribe regulations to carry out his functions, powers, and duties under this title".[Ref. 100] This is another convenient loophole if needed. Title 50[Ref. 101] deals with War and National Defense. Section 413b[Ref. 101] requires a "presidential finding"(a formal process of getting permission) before a covert action can be undertaken. This could be construed as a hindrance to OIW since many forms of it demand covertness. These two titles (10 and 50) are two good examples of the applicability of the U.S. Code to OIW.

Several other domestic documents have a role in justifying OIW. First, Executive Order 12333 [Refs 29 and 102] deals with intelligence activities in the United States. It serves as the basis for many IW decisions being made today. It gives the Director of Central Intelligence (DCI) powers to perform special assignments as dictated by the President. This could be interpreted as a vehicle for conducting some OIW operations. Second, Executive Order 12472 [Ref. 29] relates to national telecommunications during times of crisis. It provides the National Security Council (NSC) the power to allocate the nation's telecommunications systems in times of war or crisis. This statement could serve as a justification for OIW attacks launched from telecommunications platforms in the United States. Next, the Communications Act of 1934[Ref. 29] gives the President, during times of war, the power to "amend rules pertaining to wire communications". This could again serve as a basis for launching OIW attacks through that media. Finally, the Foreign Intelligence Surveillance Act of 1978[Ref. 29] allows for electronic surveillance and intelligence collection against foreign agents following a given set of guidelines. At a minimum, this act can bolster the preparations process for OIW (accurate and timely intelligence is crucial to effective OIW, a fact which will be discussed in the following section, Other Issues). The two Executive Orders and the two acts presented here clearly show the role of

such documents in Offensive Information War. Others could be found to be applicable, but the goal here is to provide a sampling, not a total list.

One can easily see that the justification for employing Offensive Information Warfare can be interpreted from several laws already enacted in the United States. However, the reverse is also true; those same laws could be interpreted as prohibitive to OIW. One might also notice that several of the items mentioned in this discussion have dealt with wartime. An OIW campaign might actually precede and preclude full hostilities. This, of course, adds to the problem of interpretation. Based on all of these ambiguities, the case could be argued for specific laws pertaining to OIW. Of course, again, this technique could backfire, and laws could be passed that prohibit the use of OIW or at least restrict it (which may not help those charged with executing OIW plans).

b. International

International laws could also be interpreted as being applicable to Offensive Information Warfare. There is no single conglomeration of international law. The closest thing to a governing body is the International Court of Justice. However, this entity only recognizes certain laws: treaties, conventions, and customary law ("law which is common to many nations"[Ref. 29]). In general, these laws are more vague (by necessity) than the laws of any given country. Also, they tend to be focused on different issues (mostly humanitarian ones) than the laws of a nation; they tend to deal with things that all of the signatories could agree to.

The deliberation here will be twofold. First, there will be a discussion of acts of war and IW. Second, various statutes and agreements (mostly drawn from United Nations sources) will be reviewed as a means to justify OIW. Naturally, not every possible portion of

international law, treaties, etc., could be examined here. Rather, the goal is to give the reader a feel for the international legal scene.

The international legal community places great emphasis on acts of war. Traditionally, declarations of war have been formal events. A series of conventions and agreements that were signed either late in the 19th or early in the 20th centuries set down the "rules" for the commencement of hostilities (*e.g.*, Lieber Code, Hague Conventions, etc.).[Ref. 103] Recently (post-World War II), this process has evolved into less formal declarations or even no declaration. However, in almost all cases, there have clearly been acts of armed force that justified a military response (in keeping with the traditions of the earlier agreements).

Warfare in the Information Age changes that paradigm. While traditional forms of warfare have included violent acts as their foundation, Information Warfare does not necessarily subscribe to that notion. Today, an OIW campaign could consist of entirely non-violent (to people) attacks. Would these attacks still be considered as acts of war and elicit perhaps an armed response? If those attacks were directed at a critical portion of the enemy's infrastructure (*e.g.*, economy), the answer is most likely yes. In such a case, would the OIW attacks be considered acts of war? This is but one of the many problems facing the international legal community.[Refs. 68, 97, 103]

Another major issue is justification. The discussion of domestic law centered around justifying the use of OIW to the people of the United States (which would be one of the primary concerns of the political leadership--recall the bulleted list from early in the chapter). The same argument must be made before the world order. As a result, an examination of some of the accepted documents in the international community should be reviewed.

Certain international legal documents could be seen as prohibitive for OIW. For example, one of the earliest arguments on limiting warfare was the Declaration of St. Petersburg in 1868. For the first time in the Western world, concern was raised about the legality and morality of certain types of weapons. The Declaration stated that using weapons "which uselessly aggravate the sufferings"[Ref. 74] of soldiers are "contrary to the laws of humanity"[Ref. 74] This document gave rise to a whole series of restrictions that became known as the Law of Armed Conflict (LOAC).[Ref. 74] This precedent could raise many questions about OIW. For example, epistemological targets could be made to undergo sufferings. But what if those sufferings were not real, but only in their minds (a real possibility in IW)? Would the LOAC still apply? This is just one of many tough issues that need to be addressed when trying to decide about employing OIW tools and techniques. Of course, there are many more examples that could be used to reiterate the prohibitive nature toward OIW of much of international law (*e.g.*, Geneva Conventions, United Nations Conventions, etc.), but are not addressed for the sake of brevity.

On the other hand, certain legal agreements could be used as a justification for OIW. For example, Article 51 of the United Nations Charter states "nothing...shall impair the inherent right of individual or collective self-defense if an armed attack occurs".[Ref. 104] If the United States' interests are attacked, this statement could be used as a justification for launching OIW assaults. If the U.S. is a victim of an OIW attack, an argument could be made that it was "an armed attack"[Ref. 104], and thus, the U.S. could respond in kind. Of course, this may not be easy, but it is possible.

In summary, knowledge of the international legal scene is crucial to any decision involving the use of Offensive Information Warfare. The statutes exist to justify OIW actions. At the same time, other (or the same) legal documents could disprove a justification claim. Care must be taken to prepare for such contingencies. Also, a lack of knowledge could lead to an unintended violation of an obscure treaty or convention.[Ref. 29] This, in turn, could result in problems with the victim nation (perhaps an ally) or condemnation from the international community.

3. Economic

A third major issue surrounding the potential use of Offensive Information Warfare is Economics. As seen in the previous chapter, OIW can have a devastating impact on national and international economies. The U.S. may not want to risk OIW attacks for three main reasons. First, the possibility exists to send the world (and thus the United States) into an economic decline by something as simple as a computer virus that was inserted at the wrong place at the wrong time. Since more and more economic transactions are being done via electronic media, the penalty for a wrong decision is rapidly increasing. Second, there may be no way to tell if a wrong decision has been made until it is too late; the nature of complex systems allows for unpredictable behavior. Finally, any attack on a country's economic system is an attack on its people. The U.S. may not want to risk losing "the moral high ground"[Ref. 97] (as discussed in the bulleted list). The economic factors mentioned here are very serious ones; the very real possibility exists of doing more damage to ourselves (due to the U.S.'s heavy involvement in the world economic order) than to the enemy.

4. Moral and Ethical

The final major issue, and the most difficult to measure, is the Moral and Ethical side of Offensive Information Warfare. As mentioned at the beginning of the chapter, the United States is perceived (mainly by its own people) as the "good guys", holding "the moral high ground".[Ref. 97] As a result, the national and international communities tend to carefully scrutinize questionable issues, frowning upon those they perceive as immoral or unethical. Many forms of OIW could fall into that category. Attacking an epistemological COG of a country, subtly subverting their will, is not "fair" (adopting the *status quo* mentality for a moment). "Good guys always fight fair, so this IW thing is not for us." Such a mentality is probably based largely on ignorance. To avoid many of these kinds of problems, an education process of some sort may be needed.[Ref. 103] However, that is a tradeoff because the U.S. may not want to reveal to its people (and thus to the world and potential enemies) the capabilities it possesses. Appealing to moral and ethical standards while waging OIW is a formidable task.

Four very tough issues have been examined in this section of the thesis. Political considerations abound in modern warfare, especially in one with an IW context. Legal issues surrounding OIW are enormous and complicated, mainly due to a lack of specific laws regarding this field. Economic issues are vital not only to the enemy but to the U.S. as well. Finally, the tough issues of Morality and Ethics must also be addressed. Resolution of these hard issues is challenging but essential.

C. OTHER ISSUES AND CONSIDERATIONS

The last section of this chapter will address other issues and considerations that must be considered when using Offensive Information Warfare. While the items discussed here may not be as lofty or potentially damaging as some of the issues discussed in the previous section, they are extremely critical nonetheless. The two basic categories presented here are "Military Issues" and "Miscellaneous Issues". One should keep in mind that there are possibly other issues and considerations that could be added if necessary. The attempt here to give the reader a feel for the vast array of things that must be addressed when contemplating the use of OIW.

1. Military Issues

The actual employment of Offensive Information Warfare is likely, at least in part, to be accomplished with some form of a military force, or at least supported by one. Thus, seven vital issues and considerations of OIW military planning and execution are presented here. They are: scope of threats, goals of attacking force, time line to hostilities, mind set of commanders, Battle Damage Indicators(BDA)/Battle Damage Assessment(BDI), levels of attacks, intelligence support, and collateral damage. Each of these is talked about briefly in the subsequent paragraphs.

a. Scope of Threats

The majority of this thesis, while not always specifically stated, has been focused primarily on large countries that are, at a minimum, well into Second Wave thinking and are embracing the Third Wave mentality (one should refer to Chapter I for an explanation of the various waves). These kinds of nations rely heavily on information and technology for survival. Of course, today's world is full of threats from smaller countries and groups that do not

necessarily fit the general mold presented in this thesis. Can Offensive Information Warfare be used against such adversaries? The answer is: yes, at least to some extent. Two examples of these non-traditional threats are Third World Countries and Sectarian Organizations.

(1) Third World Countries. Most of the conflicts that the United States finds itself embroiled in today are in developing nations. One would think that the OIW possibilities of such First and Second Wave states would be limited or non-existent. While this may be true in many cases, such things as "technology leapfrogging" (originally discussed in Chapter IV) present potential for OIW. Preparing for Third World contingencies from an OIW perspective should be a part of the planning process.

While some tools and techniques may not be appropriate in many cases, at least some form of an OIW campaign could be launched. For example, a certain underdeveloped country may not have a stock market economy, but it does have an extensive cellular phone system, complete with microwave relay towers. While an economic attack may not be possible in such a case, the cellular network could and should be prosecuted with the appropriate OIW weaponry.

While the targets here may be less sophisticated and more *ad hoc*, in some ways their vulnerability is increased. For example, a country with a primitive communications network might be a prime target for a PSYOPS campaign. Removing or subverting the existing telecommunications architecture (most likely not very complicated) should be straightforward. Due to the lack of complexity, chances are that the enemy government would be hard-pressed to refute any propaganda claims.

However, such countries present other challenges. Planning an OIW campaign requires a large amount of time when compared to other forms of warfare. Crises in Third World countries pop up all the time. Thus, planning timelines become a factor. Also, OIW requires a large amount of detailed information for planning (*i.e.*, intelligence). This may be difficult if no intelligence assets are in place when a crisis occurs. These same issues are also separate entries in this section (*e.g.*, Time line To Hostilities, Intelligence Support, etc.). One can thus see that OIW is possible against Third World countries, but it may not be feasible due to the amount of preparation required.

(2) Sectarian Organizations. Offensive Information Warfare could also be employed against Sectarian Organizations. These are such things as terrorist groups, political parties, subversive elements, etc. Obviously, the attacks would be much smaller in scope. They would most likely occur through the existing infrastructure of the country where they reside. Of course, these kinds of attacks require precision intelligence. These attacks could also result in confrontation with the host nation. Even if they are not sponsoring the organization, many attacks will probably occur through their infrastructure. These considerations may detract from the usefulness of OIW in these situations.

b. Goals of Attacking Force

The goals of the attacking force should obviously be considered when preparing OIW attacks. With the multitude of preparation and potential problems that surround this option, the U.S. leadership may opt not to utilize this powerful weapon. If the attacks can not be accomplished effectively, this is a good decision. Not using OIW because "it is just too hard" is not a valid reason. Yes, more time and effort are required for effective attacks, but the results

can be devastating. Also, OIW may be the weapon of choice in certain situations (*e.g.*, a demonstration to show a belligerent nation the potential damage that could be done to them).

c. Time line To Hostilities

As alluded to in the discussion of Scope of Threats, a large amount of time is required to prepare OIW attacks. Precision information is required. If no intelligence assests are in place to collect that information, they must be put in place. The complex nature of many modern systems requires time to learn the intricacies of them prior to targeting them. Preparation of tailored tools (*e.g.*, malicious software, sniffers, mappers, etc.) requires time. A cleverly crafted PSYOPS campaign may take years to cultivate. The weighing of the many vital issues and reaching of decisions require time. In each of these cases, a little more time is required for preparation. While rapid advances in technology may facilitate this process somewhat, a considerable amount of time will probably still be required to prepare an effective OIW campaign.

d. Mind set of Commanders

Another issue for consideration is the mindset of the military commanders. Many may just not believe or understand the potential of OIW because of a Second Wave mentality. This may translate into hesitation at the moment of truth or a poor execution of the plan. This problem is likely to be most vivid at the tactical level. For example, malicious software in conjunction with an EMP bomb is used to neutralize the fire control radars at a given air defense site. The air wing commander given the task of overflying that position may be hesitant when satellite photos show no physical damage to those structures ("How do I know those facilities are out of commission?"). Most of this mind set problem stems from ignorance. Thus, effective

education is required of at least the senior military leadership (but preferably of everyone involved). The lack of such education may be a decisive factor for determining whether or not to use OIW.

e. Battle Damage Indicators/Battle Damage Assessment

One key aspect of modern warfare is the need for timely and accurate Battle Damage Indicators (BDI)/Battle Damage Assessment (BDA). Many factors, such as increased complexity, reduced timelines, and larger battlespaces, demand a system for measuring the effectiveness of attacks. Of course, this system must be able to convey that information to the required parties accurately and in near-real time.

Information Warfare attacks raise new issues for BDI/BDA systems. Many OIW tools and techniques optimally would be precise and covert. As a result, the attacking force may know exactly where the attack took place, but how does one know if that attack was successful or not? Often, the inherent nature of such strikes (*i.e.*, covert, no control after execution by the attacker, etc.) might preclude feedback on the extent of damage that was done. For example, how does one measure how far a computer virus has spread through a network? Is the damage enough to accomplish the mission? If the possibility exists that the required BDI/BDA may not be readily available or in a comprehensive format, the decision to abort an attack or find another weapon may have to be made. For example, if a computer virus was tasked to disable an air defense system and no reliable information is available on the effectiveness of that OIW strike, a commander may decide to forgo a scheduled air raid until better information is available. Resolving BDI/BDA issues is essential for success in OIW attacks.

f. Levels of Attacks

As mentioned throughout this thesis (and incorporated into the Paradigm F discussion of Chapter II), Information Warfare can exist at the Strategic, Operational, and Tactical levels of war. As a result, OIW attacks can be directed at any or all of these components. Different tools and techniques may be best matched against one level than another. For example, a computer virus is likely to have more of an effect at the strategic level with many networked computers than at the tactical level where the network is sparse or non-existent. On the other hand, an EMP bomb is likely to have more of an effect on military telecommunications in the field than on a large network facility with much redundancy and dispersion. Also, the amount of time and preparation required for attacks at the tactical level may not be worth the effort. One can see that the level of attack is not something that can be taken for granted; it must be an inherent part of the planning process.

g. Intelligence Support

The role of intelligence support to Offensive Information Warfare is absolutely critical. Several examples of this requirement have been provided throughout this thesis. The amount and precision of information required to launch an OIW attack is enormous. The intelligence collection and dissemination entities must be familiar with these requirements and initiate activities to ensure that the required information is provided in a timely manner. This support could be anything from direction of overhead assests to placing operatives at the target source. All of these efforts require time. They also require knowledge of Information Warfare. The lack of intelligence assets or of the required details for planning may preclude the development of an OIW campaign for a given situation.

h. Collateral Damage

A final military issue that must be addressed is the possibility of collateral damage. This reality has been alluded to previously. If not carefully considered, an OIW attack can quickly go astray and cause large amounts of unintended damage, possibly to innocents or even to the attacking force. While some of this collateral damage cannot be prevented (due in large part to the nature of complex systems as mentioned previously), much of it can be alleviated by thorough preparation and effective planning. Of course, contingency plans are also always a good idea. In cases where the risk is too high for collateral damage or fratricide, the wisest plan might be to abort or postpone an OIW plan.

2. Miscellaneous Issues

To round out the chapter, the discussion will turn to several other issues or considerations that either do not directly relate to any of the other categories presented so far or are so distinct as to merit a separate, dedicated portion of the chapter. Although they are grouped as "Miscellaneous Issues", they are important to examine nevertheless. Five such issues are included here: Repercussions, Classification, Proportionality, Interoperability, and Coalitions.

a. Repercussions

Any Offensive Information Warfare attacks is likely to produce a response from the victim (if the victim knows or suspects that something has transpired). Thus, a key part of an OIW plan is a Defensive Information Warfare (DIW) plan (one may recall occurrences earlier in the thesis when the marriage of OIW and DIW were discussed). This necessity is especially important to the United States today. The U.S. is perhaps the most vulnerable of any country for OIW attacks. Although the protection is getting better, there is still a long way to go. In the

interim, considerations for possible retaliatory strikes must be planned for. Of course, repercussions need not be IW in nature; many conventional forms for revenge exist, but the U.S. is better prepared for those kinds of situations. Repercussions could also come from allies or the world community in the case of collateral damage. Before executing any OIW plan, the U.S. must be prepared to deal with any backlash, from whatever quarter.

b. Classification

Another item for consideration in OIW planning is the classification level involved. Most work within the United States government on Offensive Information Warfare is highly classified. While there are many good reasons for such safeguards, they are also inhibiting to the overall process. The case may exist that not all of the major players in an OIW campaign know what the others are doing. This is a dangerous situation. The possible results could be anything from decreased overall efficiency to calamitous collateral damage. Some vehicle for deconfliction must be in place to preclude such potential catastrophes.

c. Proportionality

The case may exist one day when the United States may have to respond in kind to an OIW attack. Before any "pre-formatted" OIW attack is launched in retaliation, care must be given to ensure the response is of the right proportion (flitting back to the legal aspects for a moment) to prevent outcry from the international community. A more difficult issue would be determining a proportionate response to a conventional attack by using an OIW tool or technique. There is simply no precedent for this type of response. As a result, there is no effective way to gauge what the proper response might be.

d. Interoperability

Interoperability issues are also important to OIW planning. If a portion of the plan is prepared by one system but will be executed by another, care must be taken to ensure that the two systems can talk to one another. Also, the path of the attack must be examined. If the attack vehicle will be passing through several systems (not necessarily controlled by friendly forces), planners must guarantee that such hand-offs can occur smoothly. This, of course, requires even more time and knowledge. While these issues may appear to be trivial, they may possibly be overlooked for just such a reason, especially in light of the myriad of other issues and considerations that are required.

e. Coalitions

A final consideration revolves around the current geopolitical scene in the world today. Rare is the occasion when the United States finds itself involved in a world conflict without some form of alliance or coalition. To what extent will the U.S. coordinate the OIW portion of its strategic plan with these allies? Failure to do so may result in collateral damage to the allied forces or at least disapproval for being left out of the loop. On the other hand, too much sharing may reveal too much about the capabilities that the U.S. possesses. After all, today's ally may be tomorrow's enemy. This is yet another tough issue that must be resolved.

This chapter has present a series of issues and considerations that must be addressed when contemplating an Offensive Information Warfare campaign. While this list of issues may not be all-inclusive, it presents a clear picture of the scope and complexity of the decisions required prior to executing an OIW plan. Of course, an examination of these issues is not as simple as going down a checklist. Many of these issues overlap or interact with one another.

The correct decision for one issue may the incorrect one for another. These are tough issues for which there are no easy answers. Yet, they must be answered, at least to some extent, before launching an OIW attack. Table 13 below is a review of the issues discussed in this chapter.

CATEGORY	SUBCATEGORY	ELEMENTS
Major Issues	Political	N/A
	Legal	Domestic
		International
	Economics	N/A
	Moral and Ethical	N/A
Other Issues	Military	Scope of Threats
		Goals of Attacking Force
		Time line To Hostilities
		Mind set of Commanders
		BDI/BDA
		Levels of Attacks
		Intelligence Support
		Collateral Damage
	Miscellaneous	Repercussions
		Classification
		Proportionality
		Interoperability
		Coalitions

Table 13. Offensive Information Warfare Issues.

VIII. CONCLUSION

A. THE THESIS IN REVIEW

This journey into the world of Information Warfare is now almost complete. A wide variety of subjects have been covered. Roughly the first half of this thesis focused on general Information Warfare ideas and concepts: definitions, players, and technologies. The second half focused specifically on one side, Offensive Information Warfare. Some tools and techniques were explored that could then be matched with the infrastructure template that was subsequently created. Finally, some tough issues surrounding Offensive Information Warfare were examined. This final chapter is broken into two parts. The first part presents a brief review of each chapter. The second part shares some thoughts and concerns the author has about Information Warfare.

1. Chapter I: Introduction

Chapter I presented the background for this thesis. The role of information in warfare was explored, from Hannibal and the Mongols to World War II and Desert Storm. During Operations Desert Shield and Desert Storm, a new dimension of warfighting began to emerge: Information Warfare. Based on some thoughts by the Tofflers about the evolution of the world towards information dependence, the Third Wave was born. An example was shown of how warfare might look in a totally Third Wave world. The discussion then reverted to the thoughts of classic military thinkers (*e.g.*, Sun Tzu and Clausewitz) and how they might be interpreted in a modern context. Other items, such as the role of technology in modern warfare and the importance of the cultural dimension, were also explored. Next, the idea of and need for Centers of Gravity was introduced. Based on all of these factors, this emerging warfighting discipline

requires a paradigm shift in thinking and, as a result, new weapons and tactics are needed. Finally, the chapter concluded with a brief synopsis of the coming chapters.

2. Chapter II: Defining Information Warfare

Chapter II focused on defining Information Warfare. The need for a definition for the purpose of speaking a common language was explored. The majority of this chapter was a series of brief overviews of many (but not all) different perspectives on Information Warfare. Included therein were definitions from national decision makers, the Department of Defense (including a definition from each of the major services), the academic world, various experts in the field of IW, and finally, some thoughts from other, less-famous people. The goal was to show how large and diverse the various definitions can be. From all of these definitions were derived two lists: things to avoid when trying to define IW and common realities from the various definitions. This lead to the discussion of Paradigm F as the context of Information Warfare for this thesis. This set of simple but powerful diagrams is a good compromise that was used in lieu of any one of the multitude of definitions that exist. The chapter concluded with some comments about the number and breadth of definitions for Information Warfare.

3. Chapter III: Information Warfare Organizations

Chapter III was a look at the various players on the Information Warfare field. From the context of Paradigm F, one could conclude that anyone could be an IW player. While this may be true to some extent, there is not much utility is saying that everyone is involved. The chapter concerned itself with a brief look at many of the more important players. They were categorized and commented on in succession. Each segment included brief comments on how, why, and to what extent the various players are involved. The four major categories were: International,

National, Federal, and State and Local. The most emphasis was placed on the National and Federal categories. The former included such entities as academia, the media, industry, and subversive elements (*i.e.*, hackers). The latter included such organizations as DOD, CIA, the Senate, etc. Most of the discussion was spent on the largest single IW participant: DOD. Each of the services, the Joint Staff, and supporting agencies (*e.g.*, NSA, DIA, etc.) were all examined. The chapter rounded out with a commentary on the lack of coordination between the various parties and the lack of clear-cut roles and responsibilities from the highest levels in this country.

4. Chapter IV: Information Warfare and Technology

Chapter IV was an exploration of some of the enabling technologies for Information Warfare. The world is undergoing a technological revolution. Advances in technology are becoming cheaper and more powerful. This chapter presented a look inside some of those technologies. While they are changing all of the time, this chapter was a good snapshot of some of the technologies that Information Warfare relies on. Four major groupings were reviewed: computers and networks (*e.g.*, proliferation of computers and networks, Internet explosion, emergence of architectures, etc.), telecommunications (*e.g.*, conventional phones, fiber optics, microwave, satellites, cellular, etc.), other pertinent technologies (*e.g.*, sensors, security, miniaturization), and emerging technologies (*e.g.*, FLAG, cognitive technologies, etc.). The chapter ended with a short discourse on the power of technology and a review of its need for Information Warfare. This concluded the first half of the thesis.

5. Chapter V: Offensive Information Warfare

The second half of the thesis focused on Offensive Information Warfare. The statement was made that no single document could examine all facets of Information Warfare. As a result,

the decision was made to focus on the offensive side. Chapter V began that exploration. The chapter was basically broken into three parts. The first part was the introduction. Although much of the work in the OIW realm is highly classified, the material in this thesis was drawn totally from unclassified sources. A brief definition of OIW was given. COGs were reviewed and targets sets discussed. The second part of the chapter discussed various OIW tools and techniques. They were split into four categories: traditional (physical destruction, electronic warfare, intelligence and information collection, and psychological operations), phreaking (traditional and cellular), computer enabled/dependent (malicious software and hacking), and technology enabled/ dependent (chipping, energy weapons, microbes, and nano machines). The final part of the chapter dealt with considerations for OIW. A method of partitioning the attack domain was presented. The bottom line of the chapter was that the United States could and should use Offensive Information Warfare.

6. Chapter VI: The Infrastructure and Information Warfare

The heart of the deliberation on Offensive Information Warfare rested in Chapter VI. This chapter dealt with the creation of an infrastructure template for using OIW. There were essentially three sections in the chapter. The first section explored the need for something such as a template. The role of COGs were explained in depth and diagrams were used to present the requirement for an infrastructure template. The second section constructed the template. The main categories were tangible and intangible. The tangible category was broken into six subcategories which, in turn, were further decomposed as shown in parentheses: political (domestic and foreign), economic (commerce and finance), industry (natural resources, agriculture, manufactured goods), essential services systems (telecommunications, power

generation and distribution, water supplies and sewage, heating and cooling, transportation, and space), geography (physical and environment), and military forces (personnel, doctrine, and systems). The intangible category consisted of three subcategories: culture, interests and goals, and history. Throughout the building of the template, specific examples and scenarios were depicted. Some of the more important elements of the template (*e.g.*, economics, telecommunications, and power generation and distribution) were defined in great detail. The last section of the chapter reviewed some commonalities inherent in many of the template elements (*e.g.*, interaction of template elements, complexity, etc.). The template thus constructed could be used by planners to wage effective OIW, when coupled with the issues and considerations of the following chapter.

7. Chapter VII: Offensive Information Warfare Issues

Chapter VII painted the last piece of the Offensive Information Warfare picture. The chapter dealt with many (but perhaps not all) issues and considerations surrounding Offensive Information Warfare. The first part of the chapter talked about the decision of whether or not to use Offensive Information Warfare. This decision must not be made on the spur of the moment; there are many complicated and tough issues that must be carefully weighed beforehand. Guiding those decisions is the *status quo* mentality that was succinctly summarized in the chapter. The second part of the chapter tackled the major issues, of which are four: political, legal (both domestic and international), economic, and moral and ethical. All of these are tough problems that need to answered satisfactorily before assent is given to launch an OIW attack. The final part of the chapter looked at some of the other issues and considerations that must be addressed when contemplating OIW strikes. These were basically broken down into two

categories: military (planning considerations) and miscellaneous (no other convenient grouping available). The former category consisted of seven elements: scope of threats, goals of attacking force, time line to hostilities, mind set of commanders, levels of attacks, intelligence support, and collateral damage. The latter category consisted of five elements: repercussions, classification, proportionality, interoperability, and coalitions. The chapter concluded with some remarks about the interaction of these issues; the problem is much larger than just going down a checklist. Still, each and every one of the issues and considerations (and perhaps others not mentioned) must be judiciously examined before a decision is made to employ OIW. There is really no other way to proceed; the price for even a small misstep could be disastrous. The end of this chapter marked the end of the exploration into Offensive Information Warfare.

B. RECOMMENDATIONS

The goal of this thesis has not been to produce the "be-all, end-all" document on Information Warfare. As stated repeatedly throughout the thesis, no single examination could possibly come close to being all-encompassing. The author does not pretend to be an expert in the field of Information Warfare. No single person could ever be an expert; the field is just too large and too diverse to allow such a specialization. The reader may disagree with any or all of the ideas presented here. As long as at least one thought was produced that leads to some kind of follow-up action, the author will feel as if the mission has been accomplished. Many of the thoughts and discussions contained in this treatise deal with complex issues. The conclusions and recommendations that are reached in this document are based on the extensive research by the author and on the author's experiences. This last part of the thesis is a series of

recommendations that the author feels will improve Information Warfare as a formidable weapon in the arsenals of the United States.

1. Education

First and foremost among these recommendations is Education. The first step in solving any problem is being knowledgeable about it. The study of Information Warfare presents unique challenges in this regard. The field is so large and so diverse and so complicated that trying to educate oneself is far from a trivial matter. Many documents exist on the subject. Almost every one presents a different view. Therein lies part of the problem.

Also, the study of Information Warfare requires a total mental adjustment on the part of the student (a paradigm shift) in order to be effective; otherwise, that person will never truly understand the power and potential of Information Warfare. Perhaps the best way to get educated is to read everything possible. This should help shape the required frame of mind. Along the way, the student will begin to formulate a conceptual view of what Information Warfare is and what it can do. Education is the first step to success with Information Warfare.

2. Definition

During the education process, one is bound to uncover many definitions (approaching infinity, one may think after wading through the literature). From that plethora of paper and electronic media, a synthesized picture is bound to emerge. The more diverse the education, the better that picture will be. This synthesized picture then becomes that person's context for Information Warfare.

One of the major problems in IW today is that everyone wants their own written definition. Unfortunately, much of this stems from squabbles over money, power, or prestige

(everyone is out to protect their own "rice bowl"). While this may be a reality of the system, some kind of compromise must be reached. A common ground must be achieved. The United States will never be effective until every major player is talking the same language; that situation does not exist today. One definition needs to be declared as the only definition. Only then will the debates cease and constructive work be accomplished.

3. Organization

Along the same lines as the definition argument, there are large numbers of organizations that have staked a claim to Information Warfare (not all of these claims are necessarily legitimate, of course). Unfortunately, there is no clear-cut guiding policy from the highest levels. As a consequence, each organization is proceeding as best as it can in the development of Information Warfare as a tool for the United States. The end result is similar to a dog chasing its tail; it may think its doing something great, but in reality it is going nowhere. The time is long past when the United States can afford such misguidance. Our adversaries are already embracing the IW potential. The very real possibility exists that unless something is done quickly, the United States may pay dearly for its floundering. The time is ripe for someone to take charge, issue the required guidance, and force everyone to conform. Although there may be some mumbling, that will quickly pass, and we will find ourselves well-equipped to enter the Information Warfare domain properly prepared and with full confidence.

4. Technology

Technology plays an important role in the development and execution of Information Warfare. The rapid explosion of technology must be cultivated quickly, in near-real time. Advances in technology must be quickly leveraged into enabling products for Information

Warfare. Traditionally, the bureaucratic process involved with taking advantage of new technology has been slow at best. Although great strides have been made recently along these lines, more needs to be done. The United States needs to be able to take advantage of a technology as soon as a breakthrough occurs. Only then will the U.S. be assured of at least remaining on par with potential adversaries.

5. Weapons and Tactics

The offensive side of Information Warfare shows great promise. Although many of the specifics regarding weapons and tactics are highly classified, thought can still be put into the possibilities. Many tools and techniques exist today in the open world, many on the Internet. While this fact presents many concerns to those charged with protecting systems from OIW-type attacks, it also presents the challenge to top those weapons. Technology will enable highly sophisticated and effective weaponry to be developed. Of course, the development of such weapons must be preceded by an embrace of the Third Wave mentality. Trying to think about OIW weapons along conventional lines (*i.e.*, Second Wave thinking) will result in the creation of very sophisticated weapons that are ineffective in the information society.

6. Infrastructure

The possibilities for the employment of Offensive Information Warfare are endless. The weapons are complex and the targets are complex. Thus, a haphazard attack plan will result only in the destruction of the attacking force and perhaps a large part of the world. OIW weapons can be so powerful as to make a nuclear detonation pale in comparison; one needs only to think of a scenario where most of the world's economic markets are destroyed by malicious software to see this power. As a result, some form of a structured methodology for devised OIW attacks is

necessary. An infrastructure template was the tool of choice for this thesis. The author makes no claim that this template is perfect, but at least it's a start in the right direction. This template is a good vehicle to present the essence of Offensive Information Warfare: vast and complex systems interacting with one another, being attacked by highly sophisticated and complex weapons in short spans of time.

The challenge now is to take the template (or something similar) and translate it into a working tool, preferably an automated one. While this may appear to be an enormous undertaking (and it is), it is also a necessary one. Even if the first attempts falter, at least something is being done. Along the way, education will occur. The final product will be an effective tool for planning and executing Offensive Information Warfare.

7. Issues

A final recommendation is aimed at the debate over issues. The decision of whether or not to use Offensive Information Warfare is not easy. No one should envy the person or persons charged with making those decisions. However, such decisions cannot be made off-hand; that would just be inviting disaster. The correct path to making a good decision is to start with a sound education base on Information Warfare, accompanied by the required paradigm shift. Included in that education is an intricate knowledge of the players, technologies, weapons, tactics, and the multitude of planning considerations. Only when all of this has been accomplished can the decision maker make a good decision. Even then, the decision made may not be the right one. Many would argue that the United States cannot afford to use Offensive Information Warfare. The argument might be that the risks outweigh the possible gains. This is most likely the result of "paradigms lost"(*i.e.*, ignorance). The world is changing. Warfare is

definitely changing. Conflict in the Information Age will be unlike anything seen in the past. It demands a new mentality to wage it successfully. One of the characteristics of the shift to the Third Wave is desensitization of human feelings. The United States has always tried to base its major decisions on what is "right". In the Information Age, such things do not exist. In order to be successful, decision makers must distance themselves from emotion and look at the decision as an efficiency problem. This may sound like a callous statement, and it is in many ways. It is also, however, reality.

This thesis has been a voyage into the expansive and complex world of Information Warfare. Much ground was covered, from definitions and organizations to weapons and issues. Many mind-numbing topics were explored. However, this work is far from complete. It has merely been a snapshot in time. Information Warfare presents great potential that should be exploited by the United States. Much pain and agony lies on the path to success. However, the journey is worth the effort. Besides, the Third Wave revolution does not leave us any choice.

LIST OF REFERENCES

1. Arquilla, J., "Warfare In The Information Age", Briefing, Department of Energy Information Warfare Conference, Naval Postgraduate School, Monterey, CA, 23 August 1995.

2. Burnette, G., "Information: The Battlefield of the Future", *Surface Warfare*, vol. 20, no. 4, 1995.

3. Campen, A., editor, *The First Information War*, AFCEA International Press, 1992.

4. "Information Warfare & Command and Control Warfare In Land Military Operations", Slides, Intelligence and Security Command, United States Army, 1994.

5. "The Information Advantage", *The Economist*, 10 June 1995.

6. Libicki, M., *The Mesh and The Net: Speculations On Armed Conflict In An Age Of Free Silicon*, National Defense University Press, 1994.

7. Toffler, A., *Power Shift: Knowledge, Wealth, and Violence at the Edge of the 21st Century*, Bantam Books, 1990.

8. Hanzhang, T., *Sun Tzu's Art of War: The Modern Chinese Interpretation*, Sterling Publishing Co., Inc., 1987.

9. Rapoport, A., editor, *Clausewitz: On War*, Penguin Books, Inc., 1968.

10. Van Creveld, M., *Technology and War: From 2000 B.C. To The Present*, The Free Press, 1989.

11. *Armed Force Staff College Publication 2: Service Warfighting Philosophy and Synchronization of Joint Forces*, National Defense University Press, 1994.

12. Gingrich, N., "Information Warfare: Definition, Doctrine, and Direction", National Defense University, 03 May 1994.

13. Hill, M., "Information Warfare", Briefing, Office of the Assistant Secretary of Defense for C3I/IW, 25 June 1995.

14. O'Neill, D., "Information Warfare", Briefing, Office of the Assistant Secretary of Defense for C3I/IW, 1995.

15. *TRADOC Pamphlet 525-69: Concept For Information Operations*, Training and Doctrine Command, United States Army, 01 August 1995.

16. "Information Warfare: Force Multiplier", Slides, OPNAV (N64), United States Navy, 1994.

17. *Cornerstones of Information Warfare*, United States Air Force, 1995.

18. *Definitions for the Discipline of Information Warfare and Strategy*, National Defense University Press, 1995.

19. Libicki, M., *What Is Information Warfare?*, National Defense University Press, 1995.

20. Arquilla, J., and Ronfeldt, D., "Cyberwar Is Coming!", RAND Corporation, 1992.

21. Schwartau, W., *Information Warfare: Chaos On The Electronic Superhighway*, Thunder's Mouth Press, 1994.

22. Campen, A., "Rush To IBW Gambles with National Security", Briefing, National Defense University, December 1995.

23. Stein, G., "Information War-Cyberwar-Netwar", Air University, 1994.

24. Garigue, R., "Information Warfare: Developing a Conceptual Framework", Office of the Assistant Deputy Minister (Defence[sic] Information Services), 1995.

25. Haeni, R., "An Introduction to Information Warfare", http://www.seas.gwu.edu/student/reto/inforwar/info-war.html, 1995.

26. Caldwell, K., "Information Warfare: The Invisible War", http://www.seas.gwu.edu/student/kimc, 1995.

27. *Memorandum of Policy No. 30: Command and Control Warfare*, Joint Chiefs of Staff, 08 March 1993.

28. Giessler, F., "Paradigm F", Briefing, National Defense University, December 1995.

29. *Information Warfare: Legal, Regulatory, Policy and Organizational Considerations for Assurance*, Information Warfare Division (J6K), Joint Chiefs of Staff, 04 July 1995.

30. De Caro, C., "Sats, Lies, and Video-Rape: The Soft War Handbook", AEROBUREAU Corporation, 1994.

31. *Random House Webster's College Dictionary*, Random House, 1991.

32. Zumstein, V., "Information Warfare: A Navy View", Briefing, National Defense University, December 1995.

33. Chief of Naval Operations, *OPNAVINST 3430: Information Warfare and Command and Control Warfare*, United States Navy, 01 April 1994.

34. McCarley, L., "Air Force Information Warfare Center", United States Air Force, 1995.

35. Cooper, P., and Oliveri, F., "Air Force Carves Operational Edge Into Info Warfare", *Defense News*, 21-27 August 1995.

36. *DOD Directive 5137.1: Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)*, http://www.dtic.dla.mil/defenselink/pubs/ofg/of_asdc3i.html, 1996.

37. Ayers, R., "DISA and Information Warfare", Briefing, Defense Information Systems Agency, 1995.

38. *Force XXI: America's Army of the 21st Century, Meeting the 21st Century Challenge*, United States Army, 1995.

39. Waller, D., "America's Persuader in the Sky", *Time*, vol. 146, no. 8, 21 August 1995.

40. Elam, D., *et. al.*, *Information Warfare: A Revolution In Modern Warfighting Concepts*, Naval Postgraduate School, 1995.

41. "Lotus NotesSuite", Pamphlet, Lotus Development Corporation, 1995.

42. Gossling, J., and McGilton, H., "The Java Language Environment: A White Paper", http://java.sun.com/whitePaper/java-whitepaper-1.html, 1996.

43. "What is the GII?", Global Information Infrastructure Agenda for Cooperation, http://iitf.doc.gov:70/0/papers/documents/giiagend.html, 1995.

44. "Defining Trends", Global Information Infrastructure Commission, http://www.gii.org/egi00063.html, 1995.

45. "NII Security: The Federal Role", National Information Infrastructure Security Issues Forum Releases, 14 June 1995.

46. Fitzgerald, J., *Business Data Communications: Basic Concepts, Security, and Design*, John Wiley & Sons, Inc., 1993.

47. *Technology Tutorials and Overviews and Vocabulary*, Global Network Intelligence, McGraw-Hill, 1993.

48. Freeman, R., *Telecommunication Transmission Handbook*, John Wiley & Sons Inc., 1991.

49. Larson, W., and Wertz, J., editors, *Space Mission Analysis and Design*, Microcosm, Inc., 1992.

50. "The Race to Global Information Super-Skyway", Mobile Satellite Services, Iridium, Inc., http://www.mot.com, 1995.

51. Wisloff, T., "A Tabulated Overview of Big LEOs", http://www.idt.unit.no/~torwi/synopsis.html, 1995.

52. Gilder, G., "Ethersphere", http://www.seas.upenn.edu/~gaj1/ethergg.html, 1995.

53. Petersonrich, R., "What is DBS?", DBS Online! Frequently Asked Questions, http://www.dss.digifix.com/DBS/DBS_Online_FAQs.htmld/index.html, 1995.

54. "GBS in JWID-95", Briefing, National Reconnaissance Office, 1995.

55. "About INMARSAT", INMARSAT, http://www.inmarsat.org/inmarsat/about.htm, 1996.

56. Garg, V., and Wilkes, J., *Wireless and Personal Communications Systems*, Prentice Hall, 1996.

57. "Cutting the Cord", *In Perspective*, http://www.witel.com/library/library.html, 1995.

58. Perkins, C., editor, "IP Mobility Support", Internet Engineering Task Force, ftp://ietf.cari.reston.va.us/internet-drafts/draft-ietf-mobileip-protocol-16.txt, 22 April 1996.

59. Leppik, P., "The Two Rules of Internet Security", Business Publications, Thinck Associates, http://www.thinck.com, 1996.

60. Braden, R., *et. al.*, "rfc1636: Report of IAB Workshop on Security in the Internet Architecture", gopher://ds0.internic.net/7waissrc:/rfc/rfcs.src?rfc1636, 10 February 1994.

61. Ranum, M., "Internet Firewalls Frequently Asked Questions", http://www.v-one.com, 1996.

62. Fulmer, C., "Firewall Product Overview", Great Circle, ftp://ftp.greatcircle.com/pub/firewalls/vendor.html, 15 February 1996.

63. Chianello, J., "Internet Doors Slam: Security Concerns Build Business Opportunity", Section F, *The Edmonton Journal*, 04 January 1996.

64. Levien, R., "A brief comparison of e-mail Encryption Protocols", cypherpunks@toad.com, 14 February 1996.

65. Denniston, F., and Runge, P., "The Glass Necklace", *IEEE Spectrum*, October 1995.

66. Deichman, S., "Future Battlefield Requires Cyberspace Warfare Strategy", *Signal*, vol.50, no. 3, November 1995.

67. Warden, J., "Employing Air Power in the Twenty-first Century", *The Future of Air Power in the Aftermath of the Gulf War*, Air University Press, 1992.

68. Kuehl, D., "Target Sets for Strategic Information Warfare in an Era of Comprehensive Situational Awareness", National Defense University, 24 January 1995.

69. Szafranski, R., "A Theory of Information Warfare: Preparing For 2020", Unites States Air Force, http://www.cdsar.af.mil/apj/szfran.html, 1996.

70. Magsig, D., "Information Warfare in the Information Age", http://www.seas.gwu.edu/student/dmagsig/infowar.html, 1995.

71. Schwartau, W., "Van Eck Radiation Helps Catch Spies", *RISKS-FORUM Digest*, vol. 15, iss. 59, http://csrc.ncsl.nist.gov/rskforum/1994/risks15.059, 26 February 1994.

72. Murray, K., "Ten Spy-Busting Secrets", Electronic Countermeasures Inc., http://www.t8000.com/eci/murray.htm, 1996.

73. Sterling, B., "The Trolls of the Pentagon", iw@all.net, 21 February 1996.

74. Cook, J., *et. al.*, "Nonlethal Weapons: Technologies, Legalities, and Potential Policies", United States Air Force, http://www.cdsar.af.mil/apj/mcgowan.html, 1996.

75. Russell, D., and Gargeni, G., *Computer Security Issues*, O'Reilly & Associates, 1994.

76. Gotts, J., "Hack FAQ", http://www-personal.engin.umich.edu/~jgotts/underground/ hack-faq-toc.html, 1996.

77. Fitzgerald, N., "Frequently Asked Questions on Virus-L/comp.virus", http://www.umcc.umich.edu/~doug/virus-faq.html, 09 October 1995.

78. Brewin, B., and Sikorovsky, E., "Hackers Storm DOD Nets", *Federal Computer Week*, 11 July 1994.

79. Lewis, P., "Internet Lets Hackers Snoop in Military Files", *The Sunday Oregonian*, 24 July 1994.

80. sikpuppy@maestro.com[real name unknown], "Re: IW Mailing List", iw@all.net, 04 February 1996.

81. Strassman, P., "Information Terrorism", Briefing, National Defense University, 10 April 1995.

82. Allman, E., at. al., "F-08: Internet Address Spoofing and Hijacked Session Attacks", CIAC Advisory Notices, http://ciac.llnl.gov/ciac/bulletins/f-08.shtml, 23 January 1995.

83. "Internet Security Services: What Needs To Be Protected?", Log-n Computing, http://www.logn.com/security.html, 05 November 1995.

84. Bacard, A., "Anonymous Remailers", http://well.com/user/abacard/remail.html, 10 November 1995.

85. Xandor, "Stick 'Ems, Slick 'Ems and Zap 'Ems", *Mondo 2000*, no. 12, 1994.

86. Strassman, P., "Selected Topics On Information Terrorism", Briefing, National Defense University, 15 December 1995.

87. *Report of the Defense Science Board Summer Study Task Force on Information Architecture for the Battlefield*, Office of the Undersecretary of Defense for Acquisition & Technology, October 1994.

88. Galvin, T., and Giles, K., "Center of Gravity: Determination, Analysis, and Application", Center For Strategic Leadership, United States Army War College, 01 September 1995.

89. *Joint Publication 3-0: Doctrine For Joint Operations*, Joint Chiefs of Staff, 1996.

90. Fadok, D., *John Boyd and John Warden: Air Power's Quest for Strategic Paralysis*, Air University Press, February 1995.

91. Turner, G., "A Nation as a System of Networks", Infrastructure Policy Directorate, Office of the Undersecretary of Defense for Policy, Briefing, National Defense University, December 1995.

92. Arnold, D., "Economic Warfare: Targeting Financial Systems as Centers of Gravity", *Challenge and Response: Anticipating U.S. Military Concerns*, Air University Press, August 1994.

93. Rinaldi, S., *Beyond The Industrial Web: Economic Synergies and Targeting Methodologies*, Air University Press, April 1995.

94. Moskowitz, B., Automotive Industry Action Group, Briefing, Internet Mail Consortium Conference, San Jose, CA, 21 February 1996.

95. Hust, G., *Taking Down Telecommunications*, Air University Press, September 1994.

96. DeBlois, M., *et. al.*, *Electronic Power Simulation (EPS): Dropping The Electric Grid, An Option for the Military Planner*, Air University Press, October 1994.

97. Morris, C., *et. al.*, "Weapons of Mass Protection: Nonlethality, Information Warfare, and Airpower in the Age of Chaos", United States Air Force, http://www.cdsar.af.mil/apj/morris.html, 1996.

98. Kievit, J., *et. al.*, "Part X: The Principle of War 'Surprise'", *The Principles of War in the 21st Century: Strategic Considerations*, http://carlisle-www.army.mil/usassi/ssipubs/pow21/pow21p10.htm, 1996.

99. Clapper, J., and Trevino, E., "Critical Security Dominates Information Warfare Moves", *Signal*, vol. 49, no. 7, March 1995.

100. "Title 10: Armed Forces", *United States Code*, http://www.law.cornell.edu/uscode/10/index.html, 1996.

101. "Title 50: War and National Defense", *United States Code*, http://www.law.cornell.edu/uscode/50/index.html, 1996.

102. Reagan R., President of the United States, "Executive Order 12333: United States Intelligence Activities", 04 December 1981, gopher://wiretap.spies.com/00/Gov/US-Docs/12333.txt, 1996.

103. Kuehl, D., "Legal Issues Related To Information Warfare", Briefing, National Defense University, December 1995.

104. "Article 51", Chapter VII, *Charter of the United Nations*, gopher://gopher.undp.org:70/00/unearth/ch6-10, 1996.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, Virginia 22060-6218

2. Dudley Know Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, California 93943-5101

3. RADM Thomas F. Stevens 1
   Commander, Naval Security Group
   Naval Security Group Activity
   Fort George G. Meade, Maryland 20755

4. RADM Harry W. Whiton 1
   Deputy Director for Policy
   National Security Agency
   Fort George G. Meade, Maryland 20755-6000

5. Bill Black 1
   NIW
   National Security Agency
   Fort George G. Meade, Maryland 20755-6000

6. Professor Dan Boger, Code CC 2
   C3 Academic Group
   Naval Postgraduate School
   Monterey, California 93943-5000

7. Professor Vicente Garcia 2
   Department of Electrical Engineering
   816 Sherman Ct.
   Marina, California 93933

8. LTC Ernest K. Beran 2
   Code 39
   Naval Postgraduate School
   Monterey, California 93943-5000

9. LTC Jeffrey A. Larsen 2
Institute for National Security Studies
2354 Fairchild Drive, Suite 5D33
U.S. Air Force Academy
Colorado Springs, Colorado 80840

10. CAPT Rocco J. Caldarella 1
Department of the Navy
CNO N64 RM 5A678
2000 Navy Pentagon
Washington, DC 20350-2000

11. CAPT Joseph T. Daly 1
Commanding Officer
Naval Information Warfare Activity
Naval Security Group Activity
Fort George G. Meade, Maryland 20755

12. Julia Wetzel 1
Commandant, National Cryptological School
National Security Agency
Fort George G. Meade, Maryland 20755-6000

13. Jim Blazer 1
Deputy Commandant, National Cryptological School
National Security Agency
Fort George G. Meade, Maryland 20755-6000

14. CAPT Lawrence C. Schaffer 1
National Security Agency (G42)
Fort George G. Meade, Maryland 20755-6000

15. Dr. Fred Giessler 2
School of Information Warfare and Strategy
National Defense University, Ft. McNair
Washington, DC 20319

16. CDR John O'Dwyer 1
Naval Information Warfare Activity
Naval Security Group Activity
Fort George G. Meade, Maryland 20755

17. CDR Chuck Williams 1
National Security Agency (G42)
Fort George G. Meade, Maryland 20755-6000

18. CDR Mike Burke 1
Fleet Information Warfare Center
2555 Amphibious Dr.
Norfolk, Virginia 23521-3225

19. John Wibbe 1
National Security Agency (N5)
Fort George G. Meade, Maryland 20755-6000

20. LTCOL K.A. Nette 1
Commanding Officer, Canadian Airborne Centre
Canadian Forces Base Edmonton
Edmonton, Alberta, Canada T5J 4J5

21. Dr. Fred Levien 1
Information Warfare Academic Group
Naval Postgraduate School
Monterey, California 93943-5000

22. Ron Wells 1
National Security Agency (W9G)
Fort George G. Meade 20755-6000

23. CPT Roger Thrasher 1
49 Carlisle Road
Transfer, Pennsylvania 16154

24. LT Donald E. Elam 20
85 Redwood Drive
Stanton, Kentucky 40380