REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	2 Jun 2000	Master's Thesis 6 Aug 99 - 2 Jun 00

4. TITLE AND SUBTITLE

United States Air Force Information Operations Doctrine: Is It Relevant?

5. FUNDING NUMBERS

6. AUTHOR(S)

MAJ James L. Griffith, U.S. Air Force

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

U.S. Army Command and Gneral Staff College
ATTN: ATZL-SWD-GD
1 Reynolds Ave., Bldg. 111, Rm. 123
Ft. Leavenworth, KS 66027-1352

8. PERFORMING ORGANIZATION REPORT NUMBER

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

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

A

13. ABSTRACT *(Maximum 200 words)*

This study examines the relevancy of US Air Force (USAF) IO doctrine, organization and training to accomplishing the Air Force's missions. This study evaluates the strengths and weaknesses of USAF IO doctrine as compared to joint doctrine and current thoughts being considered by civilian theorist and foreign nations. The discussion provides the background for answering the primary thesis research question: Is Air Force IO doctrine, organization and training relevant in today's IO environment? To adequately analyze the answer to this question, the author provides a definition of relevancy, and defines the elements that constitute the current IO environment. These definitions provide the framework upon which to evaluate the USAF's efforts in developing IO doctrine, training and organization. IO provide the edge our military needs to counter the threat of cyberwarfare, weapons of mass destruction and terrorism. The USAF must expand its capability to defend its information and information systems while simultaneously developing air power tools that contribute to the Joint Force Commander's theater IO objectives. Incorporating IO into USAF operations is the only way to maintain our edge in today's environment.

14. SUBJECT TERMS

IO, Information Operations, Information Warfare, IW, Doctrine, U.S. Air Force

15. NUMBER OF PAGES
119

16. PRICE CODE

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

UNITED STATES AIR FORCE INFORMATION OPERATIONS DOCTRINE: IS IT RELEVANT?

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

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JAMES L. GRIFFITH, MAJ, USAF
B.S., United States Air Force Academy, Colorado, 1986

Fort Leavenworth, Kansas
2000

UNITED STATES AIR FORCE INFORMATION OPERATIONS DOCTRINE: IS IT RELEVANT?

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

MASTER OF MILITARY ART AND SCIENCE
General Studies

by

JAMES L. GRIFFITH, MAJ, USAF
B.S., United States Air Force Academy, Colorado, 1986

Fort Leavenworth, Kansas
2000

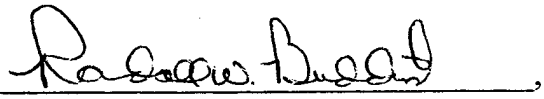
MASTER OF MILITARY ART AND SCIENCE

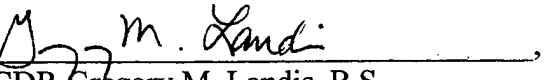
THESIS APPROVAL PAGE

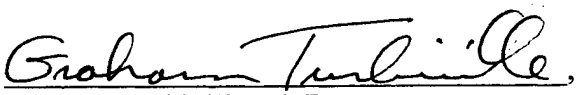
Name of candidate: Major James L. Griffith

Thesis Title: United States Air Force Information Operations Doctrine: Is it relevant?

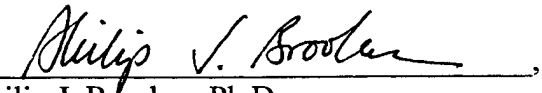
Approved by:

 , Thesis Committee Chairman
Major Randall Buddish, M.A.

 , Member
LCDR Gregory M. Landis, B.S.

 , Member
Graham Turbiville, Ph.D.

Accepted this 2d day of June 2000 by:

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

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

ABSTRACT

UNITED STATES AIR FORCE INFORMATION OPERATIONS DOCTRINE; IS IT RELEVANT? by Maj James L. Griffith, USAF, 111 pages.

This study examines the relevancy of US Air Force (USAF) IO doctrine, organization and training to accomplishing the Air Force's missions. This study evaluates the strengths and weaknesses of USAF IO doctrine as compared to joint doctrine and current thoughts being considered by civilian theorist and foreign nations. The discussion provides the background for answering the primary thesis research question: Is Air Force IO doctrine, organization and training relevant in today's IO environment? To adequately analyze the answer to this question, the author provides a definition of relevancy, and defines the elements that constitute the current IO environment. These definitions provide the framework upon which to evaluate the USAF's efforts in developing IO doctrine, training and organization. IO provide the edge the US military needs to counter the threat of cyberwarfare, weapons of mass destruction, and terrorism. The USAF must expand its capability to defend its information and information systems while simultaneously developing air power tools that contribute to the Joint Force Commander's theater IO objectives. Incorporating IO into USAF operations is the only way to maintain its edge in today's environment.

ACKNOWLEDGEMENTS

This thesis is the work of many. The sage advice of my committee advisors and several Air Force officers provided direction and purpose to this project. From the beginning Colonel Jim Gray, USAF (Retired), Colonel Swede Seagren, USAF (Retired), Colonel Jay Santee, USAF and Lieutenant Colonel Greg Crystal, USAF (Retired) provided insight into the development of Air Force and Joint information operations doctrine. Their help and advice helped immeasurably. Dr. Turbiville, Major Buddish and LCDR Landis provided insightful review of all my work and timely response to my questions and concerns. Their questions and challenges enabled me to compare my written work to the thoughts behind the words. While we did not always agree, the exercise ensured consistency of thought throughout the paper. Finally, I need to thank my wife. Sarah not only encouraged me to tackle this project, but also reviewed my work after my eyes and brain had become numb from rereading. As usual, her support made all the difference.

Any errors or fault that remain in this paper are mine alone. The views presented herein reflect my perceptions on the subject and do not necessarily represent the views of the Department of Defense or its components.

CONTENTS

FIGURE

Figure Page

CHAPTER 1

INTRODUCTION

> For to win one hundred victories in one hundred battles is not the acme of skill. To subdue the enemy without fighting is the acme of skill. (Sun Tzu, 77)

Why Write This Thesis?

Sun Tzu's well-known axiom on the pinnacle of skill in warfare may find its fullest expression in the concept of Information Operations (IO). This concept is in its infancy. However, it offers the potential to create such large asymmetries between "conventional" militaries and "information" militaries that future wars will be won by the side that dominates the information battlespace. If that is the case, it is critical that the United States (US) military take the lead in defining IO. Is it a 19-year-old computer hacker modifying a Department of Defense (DoD) home page? Is it real time information from the sensor to the shooter? Is it an F-16CJ shooting a high speed anti-radiation missile at an enemy SA-6? Is it the President of the US identifying a specific threat to national security in his State of the Union Address? It is all of this and more. IO provides a link between the national security strategy and the troops in the field. It involves the use of information technologies to provide for more effective command and control of combat forces. IO uses all the tools of national power to attack the perceptions of those who would oppose US positions worldwide. It is also THE doctrinal, organizational and training challenge facing the US Air Force (USAF) as it enters the twenty-first century. Constrained budgets, asymmetric threats, and rapid technological advancement will be the primary forces driving all of the services over the next decade.

IO may be the force multiplier the USAF requires to maintain its dominant position among world air forces.

The focus of this thesis is the manner in which the USAF is developing and implementing doctrine and organization to take advantage of the technologies available to the military today. Chapter 1 defines what IO is from the joint perspective. Joint doctrine is supposed to provide the services direction on service doctrine and organization. Joint doctrine will be the stick against which to measure USAF doctrine. Chapter 1 lays out the problem, purpose, scope, and limitations for this project. It also defines key terms used later in the project. The concepts of IO and revolution in military affairs are also addressed in Chapter 1. Chapter 1 ends with a look at the methodology used to develop the thesis.

Chapter 2 takes a broader look at IO as defined in current literature. As time passes, the concept of IO grows and matures. Current joint doctrine cannot capture all of the nuances occurring in IO and information technology today. Concepts of netwar, cyberspace, the impact of media on warfare, electronic combat (EC), and information warfare (IW) need to be evaluated for their effect on USAF doctrine and organization. The outlook of other militaries toward IO is also explored in chapter 2.

Chapter 3 defines current USAF doctrine, organization, and training for IO. The question to be answered here is: What has the USAF done to date to take advantage of new IO concepts? Chapter 3 details the baseline for recommendations and conclusions to be addressed in later chapters.

Later chapters examine the interaction of IO and information technologies and the USAF's doctrine and organization. The goal is to investigate what the USAF is doing

right and what can be done more effectively. The thesis closes out with thoughts on how the USAF can better organize and train.

Research Problem

Background

Ever since Marconi produced the first radios, nations have used them to provide for the command and control of their militaries. At the same time, their foes have looked for ways to exploit the information on the airways. As early as 1904, there is documented evidence of the Russian navy using radio intercepts to avoid the Japanese fleet (de Arcangelis 1985, 11). While the Russians ultimately lost the conflict, they found themselves in much the same position the US military finds itself today. New technologies offer new advantages and new challenges.

In 1968 Alvin Toffler wrote *Future Shock.* This book attempted to capture the impact of the then emerging computer technologies on the US society. Toffler developed a model to explain the interaction of industrialized and nonindustrialized nations. The model defined three "waves" of societal development. The first wave was agrarian, the second industrial, and the third informational (Toffler 1983, 203). Toffler's theory attempts to explain the interactions of the various parts of society in all the different waves. One of those who saw the future as Toffler did was the commander of the US Army Training and Doctrine Command (TRADOC). General Don Starry knew a change was needed in how the military conducted operations (Toffler 1993, 52).

The US military realized it needed to develop a new way of employing force in a era of unprecedented technological innovation. The roots of today's military technology challenges are found in the concepts developed in the late 1970s and early 1980s.

Technologies associated with stealth, global positioning satellites (GPS), guided munitions, JSTARS, and many others were first proposed in the post-Vietnam military. Toffler's model provided a framework within which to prepare the US Army for the approaching era of warfare. Starry's concern was that the US military was designed to function and fight as a second wave force, but the US society was becoming a third wave society (Toffler 1993, 56). The end result of the collaboration between Starry and the Tofflers was AirLand Battle doctrine.

AirLand Battle doctrine leveraged technology to create high speed, long-range power projection in a joint and combined environment (Toffler 1993, 55). The increase in the pace of information flow associated with the new information technologies provided a potential speed and lethality advantage to US forces that would overcome a numerical disadvantage in the Cold War. The doctrine was specific to the threat presented by the Soviet doctrine of echeloned forces. US forces in Europe could not stand toe-to-toe with Soviet-backed Warsaw Pact troops across central Europe. The key to maneuver warfare required by AirLand Battle was to collect, analyze, and disseminate information faster than the opposition. By knowing where to concentrate forces to take advantage of the opposition's weaknesses, the smaller NATO forces could prevail in the defense of Europe. Knowledge became the central resource for destructivity (Toffler 1993, 71). When Sadam Hussein entered Kuwait in August of 1990, the US military had the doctrine and technology to allow them to defeat the enemy they faced in central Europe.

DESERT STORM marked a turning point in military operations. In the course of the "1000-hour" war, the majority of the combat effort was exercised by airpower.

Airpower in the Gulf demonstrated the ability of technology to provide for a quick, decisive victory with minimal human cost (Jablonski 1994, 49). The tactics, techniques, and procedures used were those developed for Cold War foes. They proved effective against a less sophisticated enemy armed with modern equipment employing the doctrine of the Cold War opposition. The deciding factor was the reliance by US forces on information technology. Toffler maintains that two wars were fought in the Gulf. The first was a second wave war with dumb bombs and mass destruction; the other a third wave war with pinpoint bombing, customized destruction and little collateral damage (Toffler 1993, 67). The technologies designed in the late 1970s and early 1980s provided the knowledge required to fight a war in the information age. A new type of warfare has emerged from the Gulf War, information warfare.

In the mid-1990's, after enduring the post-Cold War drawdown, the Department of Defense (DoD) began to evaluate how the US military should be organized given the changes in the international environment. A commission was formed to review the roles and missions of all the services and service support agencies. One of the many recommendations of the commission was to organize to take advantage of information warfare as an emerging mission area (Krepinovich 1995, 3). Information technologies provide the promise of improved capability within constrained budgets. These constrained budgets are a fact of life in today's military. The military needs to be able to pack the same punch with reduced assets. Information technologies may allow the US to leverage its third wave society to maintain military dominance in a multiwave world. It also provides advantages to the primarily second wave opposition.

In his 1996 book *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Alan Campen identifies twenty-one countries that potentially had the capability to conduct information warfare (Campen 1996, 87). This list contains traditional foes, allies, and third world countries. It did not mention Yugoslavia. During the recent conflict over Kosovo, Slobodan Milosevic arguably did a better job of both internal and external perception management than NATO. Unfortunately, nationhood and leading edge technology are not required to compete in the information game. Commercially available technology can easily be added to second wave capabilities to create the weapons of information warfare (Toffler 1993, 186). The economic and technical success of the US has created the asymmetric threats that require innovative solutions in order for the US to maintain its current position in world affairs.

Problem Statement

This research project examined the adequacy of the USAF's IO doctrine, training, and organization. The project attempted to gauge the successes and shortcomings of the USAF's current posture. The paper concludes with recommendations on how the USAF can leverage IO concepts and technology to improve our ability to support the National Military Strategy in the twenty-first century.

Proponents of IO postulate a revolution in military affairs (RMA) is occurring. USAF attempts to leverage the RMA focus primarily on defending US capabilities. There is significant research on the RMA. Little research exists on how the USAF is implementing doctrine and organization to take advantage of the changes in information technology.

Research Purpose

This research project was conducted to evaluate the relevancy of the USAF's IO doctrine, training, and organization. The analysis evaluated how the USAF's doctrine and organization comply with Joint Chief of Staff (JCS) guidance on IO. It also looked at some concepts proposed by other writers for their applicability to USAF IO doctrine. The focus of the thesis was the adequacy of the USAF's IO doctrine, training, and organization.

Research Questions

The primary research question addressed in this research project: Is USAF doctrine, organization, and training relevant in today's IO environment?

Secondary questions addressed include:

1. What is new about IO?

2. What are other countries thinking about information technology and its usefulness on the battlefield?

3. Has the USAF developed the appropriate doctrine and organization to prepare the force for twenty-first century conflict?

Scope

The source of primary information was interviews with active duty and retired USAF officers who have been involved in developing both joint and USAF IO doctrine and organizations. Secondary data included available open source literature from military, civilian, and strategic think tank resources. To completely understand the issues involved in developing IO doctrine, it was necessary to examine what the other services

and civilian experts are doing in the area of IO. This secondary data forms the basis for the final analysis of the relevance of USAF IO doctrine, organization, and training.

Limitations

IO is an evolving concept. There are some commonly recognized dimensions to IO; however, there are many aspects that are not widely accepted. It is not possible to address all the dimensions of IO identified in current literature. DESERT STORM has been identified as the first war in which information age technology provided an advantage to one side over the other. While the concept of IO did not necessarily begin in DESERT STORM, US forces relied heavily on information technology to soundly defeat Iraqi forces. Immediately following the war, in an attempt to understand the impact of information in warfare, a new concept, popularly known as information dominance, was born (Johnson 1996, 4). A growing number of proponents have focused on the use of information age technology as a new field in warfare, information warfare (IW). IW, combined with the more traditional field of command and control warfare (C2), is now a new dimension in conflict referred to as information operations (IO). The evolution from information dominance to IO has occurred over the last eight years. The constant changes in terminology have confused the issues involved and made it difficult to develop a coherent sense of what IO is.

IO technology is cutting edge. New capabilities in information technology double every one and one-half to three years (Libicki 1994, 7). To stay ahead of this wave requires a massive investment in infrastructure and capability. The sensitivity of this investment induces the military to classify most of the programs directed toward IO. The

lack of open source information on new equipment, and possibly even new organizations, may impact the conclusions of this research project.

Concept Definitions

There are two concepts and several definitions that need to be addressed early in this research project. Joint doctrine is proscriptive for the services. USAF doctrine should be drawn directly from the joint directives on IO. An overview of Joint IO doctrine is included in this chapter. A more thorough review is provided in Chapter 4 as part of the review of the adequacy of USAF IO doctrine.

A term frequently encountered when reading the literature on IO is revolution in military affairs (RMA). While not critical to this paper, an understanding of the concept is important to a general understanding of the development of IO as a warfighting concept. A simple definition will not adequately address the subject area. Therefore, RMA will be briefly described in this chapter and referenced throughout the rest of the paper.

There are several operational terms that will be used frequently throughout the paper. The definitions for these terms can be found in this section. This will not be an exhaustive list, but will provide the most critical operational definitions.

Joint Information Operations Doctrine

Information operations are incorporated into almost every joint publication that addresses the operation of US military forces in conflict. The US Navy does not have a centralized doctrine document for IO. However, the Navy released *Copernicus... Forward C4I for the 21st Century* in 1995 (Davis 1997, 19). This document captures Navy thought on the application of information technologies in operations and on IO.

The Navy also included information warfare concepts in Naval Doctrine Publication 6, *Command and Control.* Navy thought on information in war and IO closely follows joint tenets, but does not include the detail provided in the joint doctrine. The US Army developed Field Manual 100-6, *Information Operations,* dated August 1996. US Army doctrine closely follows joint doctrine, but is more specific on tasks and organization than joint doctrine. The primary document defining joint doctrine on IO is Joint Pub 3-13, *Joint Doctrine for Information Operations*, dated 9 October 1998. The information in this section is from this publication.

IO is conducted by all joint force commanders (JFC) and at every level of warfare (strategic, operational, and tactical). It consists of offensive and defensive IO. IO occurs before, during, and after a conflict. The goal of IO is to enable friendly forces to achieve information superiority. This is done through the integrated use of information warfare (IW), command and control (C2) warfare, information technology, electronic warfare (EW), intelligence, and command, control, communications and computers (C4). IO also incorporates unconventional resources like civil affairs and public affairs. It is the integration of these capabilities in a timely manner that will allow the JFC to achieve information superiority. IO offers unprecedented opportunities, but also recognizes the vulnerabilities of US forces in an information dependent environment. The key to the joint doctrine is to understand the leverage cutting edge information technologies provide US forces. One problem with developing IO doctrine and organizations is the broad spectrum of tools and capabilities required to develop an integrated IO plan.

IO is doctrine developed to cope with the speed and quantity of data made available to decision makers in the age of information. IO acknowledges the impact of

both internal and external audience perception in the many stages of conflict. While the elements of IO have always been present in conflict, the speed element provided by information technology requires a concerted effort to manage these perceptions in near real time. Information technology requires new ideas about how nations will act in conflict. As one of the tools of power available to national leaders, the military needs to develop a doctrine to take advantage of the opportunities provided by the new technologies.

Revolution in Military Affairs

RMA is a concept adapted from analysis done by Soviet military writers during the Cold War. The Russians identify the need for a fundamental change in warfighting as a Military Technical Revolution (MTR). A military-technical revolution occurs "when the application of new technologies into military systems combines with innovative operational concepts and organizational adaptation to alter fundamentally the character and conduct of military operations" (Krepinevich 1997, 2). Western analyst captured this concept in the later part of the 1980s and changed the term to Revolution in Military Affairs (RMA). While there is no one definition for RMA, the Center for Strategic and International Studies defines RMA as "a fundamental advance in technology, doctrine or organization that renders existing methods of conducting warfare obsolete" (Jablonski 1994, 7). The definitions are similar, but not exactly the same. The Russian definition concentrates on the impact of technology *integrated* with new operational concepts or organizational adaptations. The more commonly accepted western definition does not require the integration.

The Russian definition more adequately explains what needs to be done to create a relevant IO doctrine and organization. Under the more accepted definition, it is possible to fixate on technology while not making necessary adjustments in doctrine or organization to leverage the new technologies. This preoccupation with technology partly explains the confusion within the field of IO today. If history is any guide, expect the current RMA to last a long time.

Under the Toffler model, the second wave culture began with the first inklings of the industrialization of the economy. Toffler identifies the search for the most effective means of mass production as the key element of the second wave society (Toffler 1993, 203). Toffler calls the concept "massification." Under the Toffler model, the last period of RMA occurred in the late eighteenth and early nineteenth century. The revolution consisted of improvements in artillery, larger, more professional armies, and the end of cavalry dominance on the battlefield (Parker 1988, 24). The seeds for this revolution were planted in the sixteenth century as the economies of the European countries began to move into the industrial period now known as the industrial revolution. The technology developed over the next two hundred years combined with the organizational changes instituted by Napoleon finally brought the RMA to fruition (Parker 1988, 147). All the developments in warfare since this time have done nothing but improve the effectiveness with which militaries can develop mass effects in war (Toffler 1993, 192). Many historians do not agree with the premise, but given the lack of integration of technology and doctrine in the most common definition of RMA, Toffler provides a viable argument. The current RMA, if indeed this is a period of RMA, may very well take as long as the second wave RMA.

Many writers feel the effective utilization of information technologies in the Gulf War is indicative of the new RMA. Toffler defines regionalized niche information based economies as the key element of the third wave society (Toffler 1993, 97). The key in warfare will be the "demassification" of the tools of conflict. The Gulf War highlighted multiservice airpower striking simultaneously across three levels of warfare with tools previously considered as only strategic capabilities (Jablonski 1994, 29). Precision guidance, advanced intelligence systems, and stealth technology allowed the allied forces to effectively attack Iraq's C2, infrastructure, and fielded forces at the same time. Whether there is an ongoing RMA is not material to the development of IO doctrine and organization. The fact is that there are many different technologies available to the ever-shrinking US forces. The US military is engaged in conflict across the entire spectrum of warfare, and it is necessary for effective doctrine to be developed to integrate new technologies with smaller forces to maintain US preeminence in world affairs.

Operational Definitions

As already indicated, IO covers a broad spectrum of ideas, tools, and capabilities. To adequately understand IO, it is necessary to speak a common language. The following definitions are not all inclusive. Definitions are from Joint Pub 3-13, *Joint Doctrine for Information Operations*, dated 9 October 1998.

Civil Affairs. The activities of a commander that establish, maintain, influence or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral or hostile area of operations in order to facilitate military operations and consolidate operational objectives.

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

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

Defensive Information Operations. The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend information and information systems.

Electronic Warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subcategories are electronic attack, electronic protection, and electronic warfare support.

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

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation.

Information Operations (IO). Actions taken to affect adversary information systems while defending one's own information and information systems.

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

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

INFOSEC. The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users.

Military Deception. Targets adversary decision makers through effects on their intelligence collection, analysis, and dissemination systems.

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

Offensive Information Operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decisionmakers to achieve or promote specific objectives. These capabilities include operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction, and special information operations.

OPSEC. Slows the adversary's decision cycle and provides the opportunity for easier and quicker attainment of friendly objectives.

PSYOP. Actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning, and ultimately, the behavior of foreign governments, organizations, groups, and individuals.

Public Affairs. Those public information, command information, and community relations activities directed toward both the external and internal publics with interest in the Department of Defense.

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

Methodology

Any review of doctrine is primarily a search for information that will prove or disprove the relevance/adequacy of current doctrine with respect to current and future threats. This research project addressed the search in three areas. The first was a search of available literature to determine the breadth and depth of IO. The process by which doctrine is developed ensures that it will always be a step behind current thought. Doctrine writers attempt to look into the future, but sometime their crystal balls are not all they should be. For this reason, it was necessary to review current military and civilian thought in the area of IO. The second area was a review of pertinent Joint and USAF publications to delimit the bounds within which the USAF develops doctrine, organization, and training. Finally, interviews were conducted with active duty and retired USAF officers who have worked in the field of IO at the joint and service level. The interviews were initially conducted via e-mail and then followed up where necessary over the phone. The interaction with people who were on the ground floor in the

military's attempt to define IO was invaluable as a tool to determine the genesis of current doctrine. Discussions with officers currently struggling with how to change military organizations in order to leverage the benefits of IO were invaluable in defining what can be done better within the USAF in the development of IO doctrine, training, and organization.

Summary

IO is a concept with such a broad portfolio, that it is easy to become confused as to the real possibilities of information technology in reforming how the military fights. Action, not words, by the services is required to move the discussion forward. This chapter laid the framework for the rest of the paper. It provided some background on the genesis of IO. The scope and limitations of the paper were defined. Operational concepts and definitions that will appear throughout the remainder of the paper were also explained and defined. Finally, the methodology used to develop ideas and information for this paper was discussed.

Chapter 2 will more thoroughly define the concept of IO. Before exploring USAF doctrine, it is necessary to understand just how broad IO really is. The discussion of joint doctrine in this chapter is only a beginning. Chapter 2 will build the basis for analysis, conclusions, and recommendations found in subsequent chapters.

CHAPTER 2

INFORMATION OPERATIONS IN THE REAL WORLD

> Knowledge is now the central resource of destructivity.
> (Toffler 1993, 71)

Keeping Up with the Pace of Change

The brief description of joint doctrine for information operations (IO) in chapter 1 provides a glimpse of how complicated this subject is. Joint doctrine focuses on the strictly military concepts of defense and offense in terms of IO. Joint IO doctrine acknowledges Alvin Toffler's concept. In order to dominate the battlefield in the twenty-first century, the warfighter must achieve and maintain information superiority. Unfortunately, joint doctrine is a compromise between the services. It is necessarily broad. To adequately judge the relevance of USAF doctrine, it is necessary to review current thought on IO. Like diplomacy, military force, and economic power, information has become a tool of national power (Stein 1999, 32). The ascendance of information technologies has generated a wide range of literature by both military and civilian writers on the use of information to achieve strategic objectives. Most of these discussions include the use of information as a tool of the military. The pace of change in concepts for the use information as a tool of national power is exceeded only by the development of new information technologies.

A fuller exploration of emerging IO concepts begins with a look at definitions of IO and information warfare (IW) not addressed earlier. The exploration continues with a discussion of the use of information at the strategic, operational, and tactical levels. One of the keys to IO in joint doctrine, as well as popular thought, is the integration of

perception management as a valid tool in conflicts at all levels. This concept is poorly defined in joint doctrine. Fortunately there is a variety of literature available in open source material on the use of the media and other tools to manage the perceptions of decision makers at all levels. Finally, it is worthwhile to look at the current trends in foreign IO doctrine. Russia and China are leaders in the development of new theories about the use of IO to achieve national objectives. Many of their early ideas were outgrowths of US thought. Since the mid-1990s, both countries have established meaningful theories within the frameworks of their cultures, economies, and technological capabilities.

Concepts and Definitions

Information Operations

Joint doctrine defines IO as "actions taken to affect adversary information systems while defending one's own information and information systems" (Joint Chiefs of Staff 1998, GL-7). While providing a place to begin, the joint doctrine does not provide a robust framework upon which to build an IO doctrine. The definition is both too broad and too narrow. It broadly defines anything done with information systems as IO. It implies narrow limits on actions conducted against an adversary. Therefore it limits its application to those times of open or covert conflict. The definition also seems to narrow the discussion to the technical systems without looking at the real utility of information in terms of national power. Information is only useful to the extent that it influences the decisions and actions of leadership. This is the human element that is ignored by the joint definition.

A broader definition of IO must encompass not only the systems required to pass information, but the human element. It must also encompass nonmilitary elements required to effectively integrate information as a tool of national power. USAF Colonel Jay Santee, US Space Command/J39, offers a definition of IO that captures the strategic nature of IO. Borrowing from the Canadian military definition, he defines IO as "actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information" (Santee 1999). Colonel Santee's definition captures the nonmilitary elements of IO. It also recognizes the target of IO is the political decision maker. The people who can impact the cessation of hostilities or prevent a conflict from ever beginning are the proper target of IO. IO is basically a strategic concept even though it has applications at the operational and tactical level. Dr. Dan Kuehl defines strategic information operations as "those military and governmental operations that protect and exploit the information environment to attain strategic objectives" (Kuehl 1997, 32). He expands his definition by acknowledging the necessity to conduct IO in peacetime as well as during conflict. George Stein defines strategic information warfare (IW) as "the battle off the battlefield. The shaping of the political context of the conflict" (Stein 1995, 33). While Stein calls this strategic IW, his concept acknowledges the political nature of information and, therefore, adds nicely to a fuller definition of IO. Peter Hill defines IO as operations to "get inside the enemy's observe, orientate, decide, act (OODA) loop" (Hill 1999, 3). The OODA loop is a concept developed by USAF Colonel John Boyd. The basic concept is to deny the enemy time to mentally cope with the pace of change in modern conflict (Fadok 1994, 19). Boyd does not define how to deny the enemy the required time, but he

emphasizes the psychological aspect of decision making in conflict. Therefore, Hill's definition of IO incorporates the human element into a definition of IO.

Based upon the preceding discussion, the author proposes the following definition: IO are actions by military and other governmental agencies to achieve strategic objectives in conflict and peace by protecting friendly use of the information environment and exploiting the information environment in order to shape an adversary's perceptions. This broader definition encompasses the nonmilitary, human, and political elements missing in the joint definition. The definition also acknowledges the role of IO in peacetime. While joint doctrine recognizes the need to conduct IO before, during, and after a conflict, the joint definition does not call out the use of IO in peacetime. The role of IO in peace is as important as in conflict; therefore a comprehensive definition of IO needs to spell this out. Finally, the definition captures the real target of IO. From dropping 1,000-pound bombs on a microwave relay tower to planting a virus in a critical computer network, the goal of IO is to manage the perceptions of those using the information. In either case, the ultimate objective is to cause the target to perceive information in a predictable manner to facilitate the achievement of strategic objectives. The proposed definition provides a more robust framework upon which to build a doctrine and organization for conducting IO.

Information Warfare

The joint definition of IW is "IO [actions taken to affect adversary information systems while defending one's own information and information systems] conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (Joint Chiefs of Staff 1998, GL-7). This definition suffers from

the same shortcomings as the joint definition of IO. Most importantly, it fails to define the target of IW.

Alan Campen gets around the problem of defining a specific target for IW by defining three types of IW. Type I IW involves managing the enemy's perceptions; Type II is denying, destroying, degrading, or distorting the enemy's information flows in order to break down his organizations and his ability to coordinate operations; and Type III involves exploiting the enemy's use of information systems in order to gather intelligence (Campen 1996, 47). This definition may be too broad, but it does capture the important elements of IW. Perceptions matter. IW can degrade an adversary's ability to act. Intelligence is an integral part of IW. Campen also provides a justification for the recent interest in IW. IW offers the opportunity to achieve military objectives with an absolute minimum of conventional force application and cost (Campen 1996, 23). Robert McGuffee defines a concept he calls information age warfare (IAW). IAW includes weapons, people, support, and C4I as employed in the information age. In McGuffee's concept, IW is a subset of IAW. IW "addresses attacks on military and 'other than military' C2 systems that have a bearing on the outcome of the conflict" (McGuffee 1999, 3). In a departure from international laws of war, McGuffee's definition acknowledges that civilian systems may be legitimate targets in IW. This aspect of IW is further supported by a definition put forward by Colonel Richard Szafranski. Colonel Szafranski defines IW as "a form of conflict that attacks information systems directly as a means to attack adversary knowledge or beliefs" (Szafranski 1995, 58). The inclusion of the adversary's beliefs brings in a stronger human element to IW than indicated in the joint definition.

Winn Schwartau defines IW as "an electronic conflict in which information is a strategic asset worthy of conquest or destruction" (Schwartau 1994, 13). Schwartau's definition captures another important aspect of IW. IW is essentially an extension of electronic warfare (EW). The joint definition of EW is "any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subcategories are electronic attack, electronic protection and electronic warfare support" (Joint Chiefs of Staff 1998, GL-6). Ultimately, most of the tools used to conduct IW make use of the electromagnetic spectrum or the susceptibilities of electronic systems to physical attacks. Under current joint doctrine the relationship between IW and EW is reversed.

Any definition of IW must include the elements covered above. The author propose the following definition: IW consists of actions taken during time of crisis or conflict to attack information systems directly as a means to alter adversary knowledge or beliefs to achieve or promote specific objectives over a specific adversary or adversaries. Accepting that non-military targets are legitimate in IW, IW doctrine needs to stress the maximum use of IW to reduce the potential costs to noncombatants of a wider conflict. IW doctrine also needs to leverage existing EW doctrine to employ IW tools in a manner that will complement the commander's concept of operations for a conflict.

Various Concepts of Interest

Outside the mainline conversations on IO and IW, there are several other concepts related to IO. The first comes from *Joint Vision 2010*. Information superiority is defined in *Joint Vision 2010* as the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do

the same (Joint Chiefs of Staff 1996, 20). In joint doctrine, information superiority is the critical enabler that facilitates the four emerging operational concepts of dominant maneuver, precision engagement, focused logistics and full dimension protection. Joint Vision 2010 goes on to say that offensive and defensive IW is essential to achieve information superiority.

Stuart Johnson and Martin Libicki propose a similar concept they call dominant battlespace knowledge. Dominant battlespace knowledge is "everything from automated target recognition to knowledge of an opponent's operational scheme and the networks relied on to pursue that scheme. The objective is to create a large gap between US forces and any opponent in awareness and understanding of everything of military significance in any arena in which we may be engaged" (Johnson 1996, 4). The key to both of these concepts is the use of information age technologies to improve our ability to dominate all spectrums of warfare. The shortcoming is that both concepts seem to limit the spectrum to the systems that process the information. To truly achieve information superiority or dominant battlespace knowledge, it is important to remember the human element.

USAF Major General Kenneth Minihan captures and expands upon the concepts of information superiority and dominant battlespace knowledge in his definition of information dominance. According to Minihan, information dominance is:

> something that is battled for, like air superiority. It is a way of increasing our capabilities by using that information to make right decisions, (and) apply them faster than the enemy can. It is a way to alter the enemy's entire perception of reality. It is a method of using all information at our disposal to predict (and affect) what happens tomorrow before the enemy even jumps out of bed and thinks about what to do today. (McLendon 1999)

By defining information dominance or information superiority as a tangible objective, it is possible to develop the tactics and procedures to achieve the condition. As air superiority is a condition that allows the USAF to control airspace when and where it chooses, information superiority will allow the USAF to control the elements of information in conflict when and where it chooses.

US military planners need to strive to achieve information superiority at the time and place of their choosing. The US military largely understands how to counter the symmetric threat on the modern battlefield. Asymmetric threats are a more troubling problem. An asymmetric strategy seeks to avoid an opponent's strengths by concentrating against their enemy's relative weaknesses (Dunlap 1999). IO offer the promise of exploiting any adversary's weaknesses without having to engage the US's larger military capability. As Iraq and Kosovo show, it is difficult to take on the US military symmetrically. As Somalia demonstrated, an asymmetric approach can be very effective. In October 1993, Somali militia was able to derail US policy by dragging the body of a US soldier through the street (Dunlap 1999). This occurred despite the fact that the US had achieved a considerable tactical victory the week prior. The Somalis could not handle the US military toe-to-toe, but they could attack public support in the US through the international media. Asymmetries work.

Another term of interest in a discussion of IO is cyberspace. According to Winn Schwartau, cyberspace is "that intangible place between computers where information momentarily exists on its route from one end of the global network to the other" (Schwartau 1994, 49). Dr. Dan Kuehl expands upon Schwartau's definition slightly in his definition. According to Dr. Kuehl, cyberspace is "that place where computers,

communications, systems and those devices that operate via radiated energy in the electromagnetic spectrum meet and interact" (Kuehl 1997, 32). The importance of these definitions is only that they provide a reference in a discussion of one part of the spectrum of conflict known as IW. Kuehl's definition is more complete because it includes not only the common understanding of networks wired together, but it also recognizes the fact that information networks of interest can travel across more traditional media. Kuehl's definition further strengthens the argument that IW is simply a new element of EW.

If the definition of IO is expanded to include perception management, then the impact of the media and, their tools, become very important. Chuck de Caro captures this element in his definition of softwar. Softwar is "the hostile use of global television to shape another nations will by changing its vision of reality" (de Caro 1997). de Caro's definition opens the possibility of using the media and media tools to bend the will of a nation and its leaders without resorting to physical force. Softwar is a critical element of IO doctrine.

Combining cyberspace and softwar concepts creates yet another concept, netwar. Netwar is "a conflict in which a combatant is organized along networked lines or employs networks for operational control and other communications" (Arquilla 1996, vii). John Arquilla and David Renfeldt expand on their definition by pointing out that netwar is "not about technology. It can be conducted over the fax, computer, phone or television. It is about organizing in a redundant way that allows for survival. The technology just makes it plausible to fight/commit crime this way" (Arquilla 1996, 15). The netwar concept helps to identify the wide spectrum of targets available to IW

warriors. There is a lot of concentration on network attack, but this may be a case of putting blinders on to avoid the need to create a more robust IO doctrine and the organizations and equipment to conduct IW. Another interesting element of the netwar definition is the mention of crime. Asymmetric threats include international organized crime, terrorist organizations, and government-sponsored groups. These organizations are all potential adversaries requiring an adequate IO doctrine to counter their threat to the US.

Strategy

IO are actions by military and other governmental agencies to achieve strategic objectives in conflict and peace by protecting friendly use of the information environment and exploiting the information environment in order to shape an adversary's perceptions. This is the working definition of IO proposed in this paper. A key point is that while IO aims to achieve strategic objectives, it has applications at all levels of operations (Jablonsky 1994, 63). IW is now seen as the more operational or tactical application of IO. The joint definition specifically calls out the use of IO in times of crisis or conflict as the definition of IW. This was not always the case.

Colonel Jim Gray was the Joint Chiefs of Staff action officer responsible for drafting and coordinating Joint Chiefs of Staff MOP 30, *Command and Control Warfare*, in 1991. In an exchange of e-mails, Colonel Gray, who retired in 1996 as the Director of Operations for the Joint Command and Control Warfare Center, provided some background on the development of IW/IO policy at the joint staff level. As MOP 30 completed the coordination cycle, TS3600.1, a top secret Office of the Secretary of Defense (OSD) policy document that defined IW, was given to Colonel Gray to

coordinate through the Joint Staff. The intent of OSD was to get IW into the popular lexicon before the end of the Bush administration's first term. The wording in TS3600.1 required a rewording in MOP 30 as well. Colonel Gray had to differentiate between command and control warfare (C2W) and IW. In his definition, C2W was military deception (the prerogative of the combatant commanders), and IW was deception (a term requiring national level concurrence of the Executive and Legislative branches of government). TS3600.1 was signed in late December 1992. Since it was a top secret document, it did not provide the majority of the people access to emerging doctrine on IW. Because of this, everyone was able to operationalize his or her own definitions of IW. IO was a replacement term for IW in order to make the concept more inclusive of the nonmilitary, governmental agencies that would need to participate in IO doctrine development. There was a great opportunity for confusion in terms.

Information has taken on a stature equal to the diplomatic, economic, and military tools of national power. National information power is the broadest range of military, governmental, and civilian information capabilities that enable national-level exploitation and dominance of the information environment (Kuehl 1997, 33). With the explosion of information technology in American culture, every aspect of American life is now susceptible to the information capabilities of any nation or even nonstate actors. A strategic attack on selected American social and economic targets combined with a coordinated psychological operation presents a relevant threat at the end of this decade that did not exist at the beginning of the decade (Howard 1994, 34). These are strategic problems, but they require a coherent strategy at all levels of operation.

The strategic level of an IO campaign aims to influence adversary choices and behavior. The operational level aims to complicate or disrupt the decision-making processes of the targeted decision maker (Szafransky 1995, 60). The tactical level includes the application of the available tools to achieve the objectives of the operational and strategic levels. Any strategy to employ IO must differentiate between the three levels of operations. Current doctrine tends to concentrate on the operational level. This is the level the military can best affect. There must be an overall strategic IO objective to give direction to the operational level of operations. It is not enough to have a campaign plan. IO should complement the campaign plan at the strategic level. To do this, IO must be coordinated at the highest possible level. Colonel Jay Santee compares current IO doctrine to the USAF doctrine for close air support. Instead of attempting to achieve information superiority like the USAF attempts to achieve air superiority, current doctrine attempts to apply IO to support individual commanders in individual engagements. As close air support is an inefficient, although sometime necessary, use of airpower, current IO doctrine is an inefficient use of information age technologies. Since the target of IO is the strategic level decision maker of an adversary, there needs to be a similar level of coordination of IO strategy in the US government.

IO is not unconstrained in application. As previously discussed IW offers the opportunity for achieving operational objectives without the level of destruction required by other forms of warfare. This kind of thinking requires a change in thought processes. Since IO occurs in peace and in conflict, the US long-standing theory of deterrence needs to change. Deterrence theory needs to give way to inducement theory (Jensen 1994, 42). Under this theory it is necessary to determine the strategic objectives desired, attempt to

shape the situation with IW applications short of force, apply force if required, and revert to nonforceful means rapidly. Under current IO doctrine, IO is simply an adjunct to the campaign, so it is not used early to influence the situation. Future IO strategy needs to consider IO earlier in the peace to conflict process.

A major constraint on IO is the ability of IO to affect noncombatants. Current US policy on the use of force requires commanders to evaluate any action based upon necessity, discrimination, proportionality, and humanity (Barnett 1998). IO does not inherently require force. Although physical destruction is a tool, it is only one of many. As recently as the Kosovo operations, this remains the policy of the US military (Graham 1999). Commanders developing the IW campaign for Kosovo were advised by the Defense Department's legal office to apply the same laws of war to IW that they applied to dropping bombs. Restraint on the use of IO is warranted, but requiring the same standard as applied to the use of destructive force will hamper the development of effective IO strategy. Information can be a meaningful tool of national power if it is judiciously applied in peacetime to deter the transition to conflict. The current IO strategy is truly IW. It emphasizes the operational level of warfare and prevents the full exploitation of the capabilities information age technologies provide the US.

Managing Perceptions

How is the current doctrine transitioned from the operational to the strategic level of warfare? IW becomes IO, and therefore strategic, by accepting the responsibility of perception management. US military thinkers are not, and should not be, comfortable with the concept of perception management. As discussed earlier, Colonel Gray had to clearly demarcate the difference between military deception and deception when initially

coordinating IW policy documents. Deception occurs with the concurrence and direction of the civilian leadership of the executive and legislative branches of government and targets the strategic level decision makers of an adversary. Military deception is part and parcel of the combatant commander's campaign plan and targets the operational decision makers. Alvin Toffler asserts that war can be won on the world's television sets (Toffler 1993, 147). Toffler encourages the military to develop the capability to distribute deceptive information, disinformation, propaganda, truth, and powerful media images. The US is still not comfortable with this role for its military. The US military cannot conduct IO without the consensus and involvement of multiple governmental agencies. If this is the case, how can the executive branch agencies be encouraged to improve the US capability to conduct IO?

The recent conflict in the Balkans provides some insight in how perception management can influence the outcome of the battle. Even before Kosovo, Slobodon Milosevic effectively employed disinformation and deceptive information to fan the ethnic flames that ignited Bosnia-Herzegovina (de Caro 1997). Milosevic was then able to use the twenty-four hour news channels to regulate the violence he inflicted on the non-Serb ethnicities in Bosnia-Herzegovina. When it looked like the American executive and legislative branches were coalescing against him, Milosevic would reduce his violence until CNN showed him he could increase the tempo. A third world dictator successfully played the international community for five years. As it turns out, the event that eventually forced Serbia to negotiate at Dayton may have also been a fine piece of perception management.

In late August of 1995, Sarajevo's marketplace was hit by 120 millimeter mortar shell (Thomas 1999). As luck would have it, Peter Jennings, of ABC news, was in Sarajevo at the time. August also tends to be a slow news month in the US. The market slaughter was headline news, and the Bosnians were quick to blame the Serbs. While no definitive proof exists that the Serbs did not launch the mortar shell, Russian Colonel Andrei Demurenko, the United Nations (UN) Chief of Staff of Sector Sarajevo, conducted an independent investigation (Thomas 1999). The UN artillery reconnaissance did not hear a mortar shell, and the colonel determined it was a "one in a million" shot to get a mortar from 3 - 4 kilometers away into a 9 meter wide alley. If this incident was not an effective use of perception management, it was truly providence for the Bosnian Croats and Muslims.

Admiral James Ellis, NATO commander of Joint Task Force Noble Anvil, the campaign against Serbia over Kosovo, prepared a commander's view brief at the conclusion of Kosovo operations. In the brief, Admiral Ellis said that the Serbians did a better job of using the press than NATO (Ellis 1999). According to the Admiral, Milosevic had "informational interior lines." Milosevic hid the atrocities being committed by his forces in Kosovo, but every time one of the NATO bombs went errant, the entire world got to see the result on the news. Secretary of Defense Cohen supported Admiral Ellis' position. Cohen felt that NATO lost the "propaganda war" (Becker 1999). Cohen asserted that even though NATO and the Pentagon attempted to restrict access to information on military operations, Milosevic was more adept at manipulating the media than NATO. According to Jamie Shea, NATO spokesman during the Kosovo conflict, NATO attempted to saturate the airwaves with their message of the day (Kitfield 1999).

NATO timed their briefings from Brussels, London, and Washington to keep the twenty-four hour media so busy they would not search for unfavorable stories. Even though Milosevic appeared to have won the tactical media war, NATO won the strategic battle over Kosovo. Against a foe more evenly matched than Serbia, the outcome could have been different.

Back to the original question: How can non-military governmental agencies be integrated into a strategic IO campaign? Kosovo was an information failure for the US and NATO. Not only did NATO lose the media war during the conflict, a Pentagon after-action report concluded that planning for regional conflicts must "reflect the full range of instruments at our disposal, including the use of economic sanctions, public diplomacy and other information efforts" (Hellman 1999). The US administration failed to fully use the power of its information tools to raise international awareness of the problems in Kosovo. No attempt was made to bring the condemnation of the UN diplomats or US citizens. The military tool was brought to bear apparently under the mistaken impression that it could solve the problem independently. This conflict provides the case study to encourage the executive branch agencies to work together to build a comprehensive IO strategy for future conflicts.

New information technologies allow planners to target specific audiences (Stein 1999). Earlier outlets like Radio Free Europe, the Cominform, Agence France Presse, and the US Information Agency were all targeted at specific, but large, audiences. With the advent of market analysis, the Internet, and world-wide news sources, information can be targeted against a specific group and continuously reinforced through multiple media. The effect of this is that a message played over and over through various sources

takes on a legitimacy all its own (de Caro 1997). Of course, this is a double-edged sword. Any organization, state sponsored or not, can gain access to the same audience the US may want to influence. This is yet another reason to create an interagency group to coordinate IO doctrine for the US. In the twenty-four hour news cycle any two-bit dictator or terrorist leader can take on the same stature as a state leader (de Caro 1997). The US must be prepared to fight this war of persuasion. The US military cannot take the lead, but the executive branch, with concurrence from the legislative branch, must organize to develop tactics, techniques, and procedures to effectively manage adversaries' perceptions if the US is to get the most from the information revolution.

Foreign IO Doctrine

DESERT STORM demonstrated the US military's ability to use information in warfare. Since that time, the US military and the US economy have become even more reliant on information and information technologies. One estimate puts 46 percent of the world's computing capacity in the US (Hoffman 1999). The Pentagon controls nearly 2.1 million computers, 10,000 local networks, and more than 100 long distance networks (Drogin 1999). This creates a lucrative target for those interested in testing their new doctrines. Just this year, the Navy's Space and Naval Warfare System's Command Center in San Diego has traced hackers to ten nations (Drogin 1999). While most of these attacks were probably just individuals, it is likely some were organized or supported by nations not friendly to US interests. The US is not the only target. Recently the Indonesian government was identified as the perpetrator of an attack on Ireland's internet provider because they hosted a site promoting independence for East Timor (Hoffman 1999). For these reasons, those who would challenge the US position in

the world are attempting to catch up to the US both technologically and in doctrine for employing IO. Of particular interest are China and Russia. Both countries are actively pursuing improvements in equipment and doctrine as a result of US success in DESERT STORM.

China is the more aggressive of the two countries. China may also be the one with the resources to actually implement their doctrine. China is convinced the US military leads the world in IW (Ahrari 1997, 472). They want to take that lead away. Writings in government- and military-controlled papers encourage the military and civilian theorists to develop asymmetrical thinking (Thomas 1998). They want to develop uncommon technologies and theories in order to get ahead of the opposition in the area of IW. Information superiority has become so important, some theorist believe it has replaced air superiority (Thomas 1998). By allowing the winner of IW to gain the initiative through control of information flows on the battlefield, IW offers the potential for a marked advantage without the risk of physical conflict. Dr. Shen Weiguang, noted as one of the first authors to write about the topic of IW, defines IW as "decision control warfare, using information as the main weapon to attack the enemy's cognitive and information systems, and to influence, check or change the decisions of enemy policymakers and their consequent hostile actions" (Thomas 1998). As discussed in this chapter, the correct target of IO is the policymaker. The Chinese realize this and are developing their doctrine to concentrate on influencing the decisions of the policymakers.

Chinese IW doctrine emphasizes both the use of information in war and the use of information as a tool to war. Information in war will allow traditional combat tools to be more effective by providing the rapid command and control and accurate targeting

information required to survive the rapid pace of the modern battlefield (Thomas 1998). The Chinese practiced this capability in an October 1998 exercise that integrated several of the military regions around the country. Information as a tool of war will allow the Chinese to attack opponents command and control elements (Thomas 1998). The application of information as a tool of war will make weapons of soft destruction more important than weapons of hard destruction. An article in the *Liberation Army Daily*, the official daily newspaper of the People's Liberation Army General Political Department, stated that it was essential to develop capabilities including information-paralyzing software, information-blocking software, and information-deception software (Gertz 1999). The same article postulated the creation of a new force of equal stature to the Army, Navy, and Air Force. China is reportedly already developing some offensive IW weapons. China may already have lasers that can blind optical sensors in US satellites. They are also reported to be developing a capability to interdict GPS signals (Newman 1999). These capabilities alone would allow them to blind US ability to track movements and to accurately target. GPS is becoming the information tool of choice to allow smart bombs to kill one target with each bomb. The loss of this capability would require more sorties to kill each target. Obviously, the Chinese are aggressively pursuing their capabilities.

The *Economist* magazine reported that the Chinese launched 72,000 cyber attacks against Taiwan in August 1999 (Christenson 1999). The Taiwanese struck back by attacking the computer networks of the Chinese tax and railway agencies. Following the bombing of the Chinese Embassy in Belgrade during the Kosovo conflict, the Chinese government reportedly launched several attacks on US government computer networks

(Hoffman 1999). This attack managed to disrupt some public access web pages, but also revealed 3,000 to 4,000 back doors into US computer systems that had been designed by China. The implication of these back doors is more alarming than the attack. Software and computer systems are developed all over the world and then integrated into systems all over the world. Any country interested in conducting an organized attack on commercial or military computer networks could simply bury a virus in commercially available software and wait. The impact of the virus would be dependent on the popularity of the application, but could be sizeable if the software was popular enough. Even more important, it would be very difficult to trace the source of the original virus. China demonstrated the capability to conduct this kind of IW with the discovery of the computer back doors. China has grasped the importance of IO. Their military is leading the charge to improve not only the physical capabilities to defend and attack information, but also the theoretical underpinnings they hope will allow them to surpass the US in the ability to achieve information superiority.

Russia has less capability to conduct IO, but has had a greater effect on the development of US IO doctrine. Much of what the US military did in DESERT STORM can trace its origins to the Soviet doctrine of reconnaissance-strike complex. The reconnaissance-strike complex concept involves providing aircraft and artillery multi-sensor reconnaissance information to identify and geolocate targets so that the shooters can employ precision weapons (Dick 1993, 390). The Soviet military was not able to develop the technologies to execute this concept prior to the end of the Cold War. The US was able to develop much of the technology to execute the concept, but did not achieve the real-time feed the concept envisioned. Much of the information technology

developed since the Gulf War is designed to close the time gap in the current capability. The Soviets also developed a concept that leveraged information as a tool of war. The concept is known as radio electronic combat (REC). REC encompasses electronic warfare and perception management (Munro 1991, 134). The REC concept was intended to hide secrets and pass misinformation in peacetime and war. The military deception element of REC is encompassed under the term maskirovka. Maskirovka combines deception, camouflage, and disinformation at all levels of warfare to protect military capabilities (Bunker 1996, 66). The Russians continued the Soviet preoccupation with REC by raising forces assigned to perform the military REC functions from a combat support function to special weapons status (Dick 1993, 390). The Russians learned from the Gulf War that you ca not win the ground war if you do not win the air war and gain electronic superiority. Even though the Soviet's had a doctrinal head start, their emerging IO doctrine borrows heavily from US thought.

Russia's ability to effectively employ their revolutionary REC and reconnaissance-strike complex doctrines was severely hampered by the culture of the Soviet Union. The communist government of the Soviet Union maintained an inflexible grip on all information systems (Thomas 1996). The spread of information technologies threatened the government and was officially forbidden by General Secretary Nikita Khrushchev in the 1950s. Since the end of the Cold War, the Russian government has been unable to maintain tight control. In fact, software and hardware piracy are rampant in Russia (Thomas 1996). The proliferation of information technologies will allow the Russians to rapidly catch up with the west in competency with information systems. This rapid change provides both an opportunity and a threat to Russia. The opportunity is an

increase in productivity driven by the efficiency gained from adapting information age technologies to the Russian economy. The threat is a growing dependence on networked computers to run the various components of the economy, government, and military.

Russia has responded to this threat by developing IW doctrine. Although there is not one authoritative definition of IO/IW for the Russian military, Admiral Vladimir Pirumov, the Scientific Advisor to the President of Russian, defines IW as

> a new form of battle of two or more sides which consists of the goal-oriented use of special means and methods of influencing the enemies information resource, and also of protecting one's own information resource, in order to achieve assigned goals. An information resource is understood to be information which is gathered and stored during the development of science, practical human activity and the operation of special organizations or devices for the collection, processing and presentation of information saved magnetically or in any other form which assures its delivery in time and space to consumers in order to solve scientific, manufacturing or management tasks. (Thomas 1998)

The definition is very broad, but it captures the concept of protecting one's own information, attacking the opponent's information and targeting the human element. The definition also does not limit the use of IW to periods of conflict. There are many more definitions available, from both military and civilian sources, but the themes in all are the same as the definition provided. When combined with the earlier doctrinal concepts of REC and reconnaissance-strike complex, the Russians have a robust IO doctrine.

In the Russian view, the center of gravity in military operations has shifted from land and sea to air and space (Thomas 1999). Information technologies have sped up the decision cycle on the battlefield and will require decision makers to be able to react to events, on and off the battlefield, more quickly than in the past. Russia is concentrating its IW/IO efforts in several different areas. The first is security of its own systems. In 1993 the Federal Agency for Government Communications and Information was founded

to counter hackers, intelligence collection efforts over networked systems, and criminal use of the internet (Thomas 1999). Next, the Russian military is developing doctrine to allow it to more effectively employ their perception management concept of reflexive control. Reflexive control is "a means or method used to convey specially prepared information to a person, organization or country to influence the adoption of predetermined decision desired by the initiator of the action" (Thomas 1999). While reflexive control is a concept developed during the Soviet era, new information technologies and media outlets offer the opportunity for a more effective application of the doctrine. A related area of interest to the Russians is protection of their citizens from perception management attacks. As Russia transitions from the Soviet model to whatever its next period will be, the citizens are psychologically vulnerable (Thomas 1999). The Russian government and military want to actively defend against this threat until Russian society is able to find more solid ground. For Russia, IW is a strategic, operational and tactical threat (Thomas 1998). Russia is actively pursuing increased capability and can be expected to be a threat to US computer networks.

A recent incident captures the potential threat Russia poses to US networked computers. In an operation dubbed Moonlight Maze, hackers from the Russian Academy of Sciences are believed to have accessed sensitive science and technology from Department of Defense computer systems (Vistica 1999, 52). While the incident cannot yet be directly tied to a coordinated assault by the Russian government, it is possible that classified missile codes and information on missile guidance systems were compromised in this attack. As a result of this attack, the Department of Defense ordered all of its civilian and military employees to change their passwords. The Russians have denied

any involvement in the incidents. According to Anton Nossik, chief editor of a Russian online daily newspaper, *Gazeta.ru*, the Russian government has cooperated with the US Federal Bureau of Investigation as it attempts to identify the perpetrators of the Moonlight Maze attacks (Verton 1999). With over 1.7 million internet users in Russia, it is possible the incident was the work of someone who hacked into the Russian Academy of Science computers and then used them as a conduit into the US systems. Whether it was a coordinated attack by the Russian government or a case of skilled hackers trying to put the blame at the Russian's doorstep, the Moonlight Maze incidents provide a window into the susceptibility of US civilian and military systems to a determined opponent.

As the availability of information technologies increase in Russia, the Russian government becomes more concerned about the threat this poses to their population. As discussed earlier, the Russian people are in a period of transition. Until this transition is complete, they may be vulnerable to a psychological attack using the various information means now available in Russia. Moscow is trying to build support for a UN resolution to set international guidelines on the use of information weapons (Graham 1999). The US sees Russian efforts in this area as an attempt to stall US development of new weapons. It is likely that the US will continue to lead the Russians significantly in their ability to conduct IW.

The Russians have led in the development of doctrine to employ information technology. Under the Soviet system they were unable to turn theory into practice. In their current economic and cultural condition, the Russians are still attempting to lead in the development of IW, but do not currently possess the technological ability to turn

theory into practice. As Russia emerges from its transition period, if it does, the US must prepare to counter them in the information spectrum.

Summary

This chapter more thoroughly defined the concept of IO. Before exploring USAF doctrine, it was necessary to understand just how broad IO really is. The discussion of IO/IW doctrine in this chapter provides a more robust framework against which to measure USAF IO doctrine. It is plain that there is still much confusion as to what IO and IW are. I have proposed a working definition for both concepts. These definitions will build the basis for analysis, conclusions, and recommendations concerning USAF doctrine found in chapters 4 and 5. IO makes use of information at the strategic, operational, and tactical levels. The key component missing from the US joint definition of IO is the integration of perception management as a valid tool in conflicts at all levels. The chapter closed with a look at the current trends in foreign IO doctrine. Russia and China are leaders in the development of new theories about the use of IO to achieve national objectives. Many of their early ideas were outgrowths of US thought. Since the mid-1990s, both countries have established meaningful theories within the frameworks of their cultures, economies, and technological capabilities.

The next chapter will review USAF IO doctrine, organization, and training. The basis for this chapter will be Air Force doctrine documents, speeches and writings of USAF leaders, and open source literature on the USAF's IO programs. The later chapters of the paper will evaluate the relevancy of the USAF's doctrine, organization, and training as it enters the twenty-first century.

CHAPTER 3

AIR FORCE DOCTRINE

> Air and space doctrine is a statement of officially sanctioned beliefs and warfighting principles that describe and guide the proper use of air and space forces in military operations. (AFDD 1 1997, 1)

In the Beginning

Doctrine institutionalizes current concepts about how an organization plans to utilize its unique characteristics, resources, and opportunities to achieve common objectives. Written doctrine is simply a snapshot in time. Frequently service doctrine is out of date before it gets to the field. It is, however, critical to provide an organization as large as the USAF with coherent, relevant doctrine. Doctrine usually begins with a lessons learned from observations and experience. These lessons generate ideas, either from the top or the bottom of the organization, which attempt to explain an emerging trend or characteristic. The initial idea will usually begin a discussion. The discussion will play itself out in unofficial channels, initially, and then find its way into official literature. Eventually, the idea achieves official acceptance and support and becomes doctrine.

USAF IO doctrine sprang from ideas generated by the astounding success of coalition forces in DESERT STORM. These ideas initially found their official, joint expression in the doctrine of command and control warfare (C2W). USAF thinkers felt that C2W did not completely explain the force multiplication effect produced by the integration of information technologies and existing tactics, techniques and procedures (Tirpak 1997). C2W was an evolutionary concept. As discussed in previous chapters,

many thinkers feel DESERT STORM demonstrated revolutionary changes. The USAF needed a doctrine that not only captured existing capabilities and ideas, but a doctrine that could incorporate new technologies and guide the application of concepts into revolutionary capabilities.

This chapter will look at the genesis of USAF IO doctrine. Seven years passed from the end of DESERT STORM to the completion of the initial Air Force doctrine documents (AFDD) on IO. Seven years is not an excessive length of time to develop doctrine. The idea of integrating information technologies to create an asymmetric advantage for US military forces was born before the 1991 war against Iraq. DESERT STORM simply demonstrated the potential offered by asymmetric strategies. This chapter will explore the development of USAF IO doctrine from a new idea to an officially sanctioned belief or principle. From doctrine flows organization and training. This chapter will also look at how the USAF has adapted its organization and training to incorporate IO into the mainstream of USAF operations.

Discussion

In chapters 1 and 2 there is considerable discussion on the origin of IW concepts in both military and civilian circles. The work of Alvin and Heidi Toffler with TRADOC in the late 1970's and early 1980's helped define a coherent Army and USAF doctrine that made use of emerging information technologies to improve the ability of US forces to counter an enemy that was significantly larger. At the same time, the USAF invested billions of dollars in stealth technology, EW capability, and improved airborne command and control capabilities. All of these steps were evolutionary in nature. DESERT STORM pitted the US military against an enemy of approximately equal size. Despite

relative equality in force quantity, the US military was able to achieve success at an incredibly low cost in resources and personnel. Immediately, theorists attempted to identify the reasons for the success of the US military. The seeds of IW are found in this search for an answer. Unfortunately, most of the work was done at a classified level and little is available on the thoughts of those developing initial IW doctrine.

In 1994 General Merrill A. McPeak, then USAF Chief of Staff, directed Major General Robert E. Linhard, then director of Plans in the office of the USAF Deputy Chief of Staff for Plans and Operations, to formulate a USAF IW doctrine. General Linhard relates that when they came back with their proposed doctrine General McPeak felt their proposal was too evolutionary. The Gulf War had demonstrated the revolutionary potential of information and information systems. General McPeak was looking for a more encompassing strategy that captured the synergy offered by new technologies and the effect on an adversary's ability to wage war when they could not trust their own information (Tirpak 1997). General McPeak also directed that IW be incorporated into USAF operations. He did not want another stovepipe organization. He wanted a tactical and operational level doctrine. The USAF would let someone else worry about the strategic aspects of IW (Tirpak 1997).

Also in 1994, Colonel John A. Warden III, a recognized airpower theorist, published his thoughts on the future of air theory. Colonel Warden anticipated the prominence information would take as military theories for the new century began to unfold (Warden 1997, 1). Warden felt the lessons about information from the Gulf War were negative (Warden 1997, 12). While the coalition successfully broke the Iraqi's ability to communicate information in both military and civilian environments, the allies

failed to offer the Iraqi's an alternative source of information. Colonel Warden recognized the true nature of IO at a very early stage in the development of USAF doctrine. It is not enough to deny the adversary information. Military planners must be prepared to provide an alternative source of information that supports friendly objectives. Warden also argued that it was time for US forces to reorganize to exploit the new information technologies.

In the early 1990s the USAF took steps to reorganize. The USAF Electronic Warfare Center was reorganized as the Air Force Information Warfare Center (AFIWC) in September 1993. The mission of AFIWC was to anticipate IW offensive and defensive capabilities, organize and execute IW exercises, and integrate IW into other exercises. As part of this organization the USAF also began developing the air operations center (AOC) concept. The AOC would provide a single correlation node for information entering the theater from multiple sources (Tirpak 1997). The idea was to create information useful to the commander from all the data being provided by sources outside the theater. The AOC concept recognized the fact that more information could be available to the commander than the commander could use.

In 1995 General Ronald R. Fogleman, then USAF Chief of Staff, directed the establishment of the 609th Information Warfare Squadron at Shaw AFB, South Carolina. The 609th was the first IW dedicated unit of any military service (Tirpak 1997). General Fogleman was concerned that there was no single point of contact for IW and that there was no coherent doctrine for the development of the emerging computer network attack (CNA) mission (Crystal 1999). The 609th belonged to Air Combat Command and was, therefore, an operations unit. Personnel for the squadron came from intelligence,

computer, communications, and EW backgrounds. Ultimately the squadron was disbanded. There are several reasons for the short tenure of the 609th IWS. The bottom line is that the squadron was never properly manned and no coherent doctrine existed for its mission. The squadron was, however, a first attempt to organize an operational IW unit.

1n 1995 and 1996 Dr. George J. Stein, then director, International Security Studies core and professor of European Studies at the Air War College, Maxwell Air Force Base, wrote on IW. Dr. Stein expressed IW concepts more in line with what is today called IO. He postulated that IW was the "emerging theater in which future nation-against-nation conflict at the *strategic* level is most likely to occur" (Stein 1995, 30). While the work done by General Linhard at the Air Staff a year earlier left the strategic concepts to someone else, Dr. Stein identified the strategic nature of IW. He defined IW as: "actions taken to achieve relatively greater understanding of the strengths, weaknesses, and centers of gravity of an adversary's military, political, social, and economic infrastructure in order to deny, exploit, influence, corrupt, or destroy those adversary information-based activities through command and control warfare and information attack" (Stein 1996, 1). Dr. Stein identified the essential element of IW as the ability to influence human beings and the decisions they make. He said, "The target of information warfare, then, is the human mind, especially those minds that make the key decisions of war or peace and, from the military perspective, those minds that make the key decisions on if, when, and how to employ the assets and capabilities embedded in their strategic structures" (Stein 1995, 31). He supported the concept as expressed by Colonel Warden in 1994.

Dr. Stein identified the information environment as equal to air and space environments. He saw the extension of existing USAF doctrine into this new environment. Superiority in the information "realm" was as important as air superiority and space superiority to achieve strategic objectives. He saw the concentration on the evolutionary concept of information-in-war (IIW) as the greatest danger to the full development of a revolutionary IW strategy (Stein 1995, 38). He was concerned that the vital information functions required to conduct effective combat operations (the definition of IIW) in a modern military would override the development of effective tools for conducting IW (Stein 1996, 21). Dr. Stein was leading the way in the discussion of USAF IW concepts.

At the same time Dr. Stein was recommending strategic ideas on IW, new evolutionary concepts for employing information technologies to improve USAF operations were being developed. One of these concepts was known as real-time information into the cockpit (RTIC). The concept built upon the Russian reconnaissance-strike complex concept. RTIC offered the hope of streamlining the process of providing aircrew with timely, accurate off-board information to allow for more effective targeting (Chapman 1997). The concept leveraged existing information collection and dissemination platforms (airborne and ground based) to rapidly identify, locate, and target high priority targets in a specific theater. In DESERT STORM, US sensors could identify SCUD launches, but could not provide accurate enough information to the airborne strike aircraft to allow them to target the mobile missiles. RTIC technologies would allow the information to be transferred from the information sensors to the attack aircraft without a delay for security or accuracy reasons. An added advantage of the

RTIC concept is that the commander in the AOC would be receiving the same updates and could more effectively manage limited airpower assets. In July 1995, ACC and the Space Warfare Center conducted Project Strike I to demonstrate the validity of the RTIC concept. While not a complete success, the test demonstrated the technologies to tailor intelligence to ongoing strike missions, to pass near real time (NRT) information to strike aircraft, to process and display NRT information on the strike platform, to conduct a successful strike based upon the information provided and to allow the commander to tailor intelligence and threat data for direct dissemination to tactical platforms (Chapman 1997). The Russians developed the reconnaissance strike concept in the early 1980s. SCUD hunting in the 1991 Gulf War identified a serious shortfall in capability and a demonstration of capabilities was conducted in 1995.

As demonstrated in this section, USAF discussions on IW were being conducted at all levels of the organization and in multiple disciplines. With the amount of interest generated by IW, it was inevitable that the discussion would move from unofficial to official channels. In 1995 General Fogleman authorized the release of the first official document on IW doctrine for the USAF.

Cornerstones of Information Warfare was released under the signature of General Fogleman and Secretary of the Air Force Sheila E. Widnall. The paper was not doctrine; it described how IW doctrine should be developed (*Cornerstones* 1995, 1). There were several ideas espoused in *Cornerstones*. The paper discussed the transformation in warfare caused by the rise of information technologies and for the first time delineated a difference between IIW and IW. IIW allows combat operations to proceed with unprecedented economies of time and force (*Cornerstones* 1995, 2). IW foresees the use

of information as both a weapon and a target. Most of the discussion to this point had revolved around IIW. *Cornerstones* opened up the field of IW to offensive action and separated IW from the use of information-in-war.

The paper defines IW 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" (*Cornerstones* 1995, 3). The definition carefully separates effects from means. Previous concentration had been on information technologies. *Cornerstones* proposed a concept that adopted current and future technologies into an integrated operation to achieve the effects necessary to establish information superiority. The paper expanded upon the then traditional view of information as a force multiplier. Information in USAF terms was now also a weapon.

In *Cornerstones*, IW is comprised of the more traditional functions of psychological operations, electronic warfare, military deception, physical attack and operations (OPSEC), communications (COMSEC), and computer security (COMPUSEC). Additionally, the concept of information attack is introduced. Information attack is defined as "directly corrupting information without visibly changing the physical entity within which it resides" (*Cornerstones* 1995, 6). Information attack provides both direct and indirect attacks to alter the information upon which the adversary makes decisions. Indirect attacks create information that misleads the adversary. Military deception, OPSEC, and physical attacks achieve results indirectly by creating an apparent reality for the adversary to observe, orient, and react to in a desired manner. Direct attacks alter components without the adversary having to interpret or perceive new information. Direct attacks place the information in the adversary's

information system without the adversary needing to collect or evaluate the data. The adversary is passive in a direct attack. Either form of information attack relies upon attacking the information without the adversary perceiving any physical changes.

Cornerstones also addresses incorporating IW into existing USAF doctrine. The doctrines of air and space power are built upon these elements: control, exploit and enhance. The paper proposes a similar construct for IW doctrine. IW will "control the information realm so we can exploit it while protecting our own military information functions from enemy action; exploit control of information to employ information warfare against the enemy; and, enhance overall force effectiveness by fully developing military information functions" (*Cornerstones* 1995, 9).

USAF doctrine recognizes counterair and counterspace as control missions for air and space power. *Cornerstones* added a third control mission, counterinformation. Counterinformation, "actions dedicated to controlling the information realm," has both an offensive and defensive components (*Cornerstones* 1995, 9). Offensive counterinformation includes physical attack, military deception, psychological operations, EW and information attack. Defensive counterinformation includes physical attack, physical security, hardening, OPSEC, COMSEC, COMPUSEC and counterintelligence.

Air and space power exploits control through strategic attack, interdiction, and close air support. IW can achieve the same effects as the counterair exploitation missions using the information realm (*Cornerstones* 1995, 9). The applicability of this element in the counterinformation role depends upon the reliance of the adversary on automated control for priority infrastructure items. The paper also recognizes C2 attack as a new

force application to exploit control. C2 attack is " any action against any element of the enemy's command and control system" (*Cornerstones* 1995, 10). DESERT STORM proved the value of targeting C2 nodes to blind an adversary or alter the adversary's perception of the environment. *Cornerstones* captured that lesson as part of emerging USAF IW doctrine.

Air and space power enhance force effectiveness through the applications of airlift, air refueling, spacelift, and special operations. IW enhances force effectiveness through the application of information operations (IO). In *Cornerstones* IO are "any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces" (*Cornerstones* 1995, 11). In the USAF's emerging IW doctrine IO was a force enhancement application of IW.

Cornerstones not only addressed the emerging concept of IW, it redesigned the construct upon which air and space power doctrine was developed. IW subsumed electronic combat and IO subsumed surveillance and reconnaissance (*Cornerstones* 1995, 11). The paper changed the paradigm in order to integrate IW into all USAF operations. Familiar constructs allowed the USAF to more rapidly incorporate IW thought into mainstream USAF operations.

The USAF stepped out in 1995 to embrace the concepts of IW espoused in the *Cornerstones* paper. In a speech presented 16 May 1995, General Fogleman defined IW as the fifth dimension of warfare (Fogleman 1995). According to the General's remarks IW are actions taken to exploit information on the enemy; to deny, corrupt, or destroy the enemy's databases; and to protect friendly systems. Under this construct it was possible to achieve desired effects in a different way from those used in the Gulf War. The

General suggested that, by viewing the enemy's information activities as a system, military planners would be able to make trade-offs between lethal and nonlethal methods not available to US forces during the Gulf War. General Fogleman also touched on adjustments made to training under his tenure. IW training was incorporated into intermediate and senior service schools at Maxwell Air Force Base, Alabama. IW training was also provided to the numbered air force (NAF) staffs. NAFs are the operational level staff in the USAF organizational hierarchy. Finally, the general talked about how IW was being incorporated into USAF acquisition programs. Under his watch, all new weapons system procurements had to meet a requirement for information security. General Fogleman was a driving force behind the development of USAF IW doctrine.

In May 1996, Major General Charles D. Link, then USAF assistant deputy Chief of Staff Plan and Operations, forwarded a RAND Issue Paper written by Glenn Buchan of RAND to all USAF general officers. General Link forwarded the paper at the request of General Fogleman. Glenn Buchan addresses many of the ideas already covered in this section. He did, however, propose a couple of new ideas. First, Mr. Buchan recommended the USAF concentrate on integrating IO, as defined in *Cornerstones*, into all its operations and organizations (Buchan 1996, 5). The next priority, according to Mr. Buchan, was to reduce the vulnerability of USAF information systems. As an example Mr. Buchan referenced the results of a Defense Information Systems Agency (DISA) exercise against 8,000 unclassified DoD computers. DISA was able to access eighty-eight percent of the computers; only five percent of the system administrators detected

the unauthorized access and only 5 percent of those reported the intrusion (Buchan 1996, 6). While the USAF did better than the other agencies tested, the exercise amply demonstrated the vulnerability of USAF information systems. With the USAF's growing dependence on information systems, protecting those systems is critical to effective combat operations.

The most interesting idea put forth by Mr. Buchan concerned the planned investment in IW technologies. Mr. Buchan recommended a broad assessment be conducted of potential adversaries' vulnerability to information attacks (Buchan 1996, 8). If potential foes are not vulnerable, why expend the resources to develop the information technologies to attack them? The issue paper points out that information attack technologies are fragile because information systems are easily patched when a weakness is detected and information systems tend to mutate into nonstandard configurations. With each system being individualized, it is necessary to develop system specific attack routines. For this reason Mr. Buchan recommended information attacks, attacks targeted against computer-based information systems, take place in conjunction with more conventional physical or electronic attacks (Buchan 1996, 9). This would allow fewer computer systems to be targeted by CNA and, therefore, require fewer of the scarce CNA resources available to a commander. Organizational change would be required in order to incorporate these new ideas into mainstream USAF operations.

Mr. Buchan recommended a couple of organizational changes. He suggested establishing information-related career paths within the existing force structure (Buchan 1996, 9). Mr. Buchan felt this would prevent IW from being marginalized by the operational force. He also endorsed the USAF decision to give USAF/XO (Plans and

Operations) and Air Combat Command (ACC) the lead in IW. XO and ACC are operational organizations able to operationalize IW in USAF operations. Mr. Buchan's ideas continue a trend towards preventing IW from being stovepiped behind classification and technical "green" doors. The worth of all these discussions is found in their ability to withstand the intellectual review conducted prior to the release of new doctrine.

Doctrine

The jump between discussion and doctrine is not often a giant leap. *Cornerstones for Information Warfare* laid out the construct for the integration of IW doctrine into USAF operations. *Cornerstones* was published in 1995. USAF doctrine began to reflect its impact in 1997. USAF doctrine is captured in a series of AFDDs developed by the USAF Doctrine Center at Maxwell Air Force Base, Alabama.

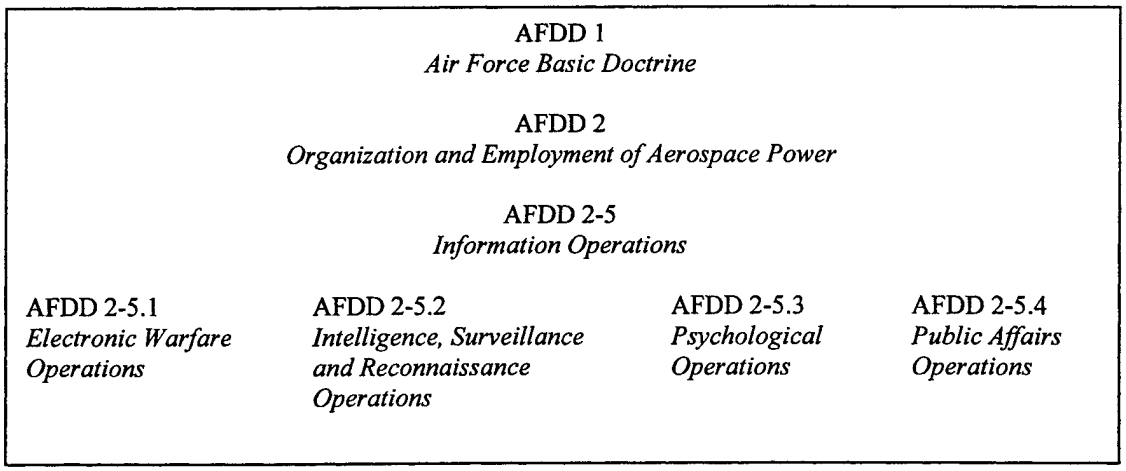


Figure 1. Air Force IO Doctrine Documents

Figure 1 depicts the USAF doctrine documents pertinent to IO. AFDD 2-5.1, AFDD 2-5.2, AFDD 2-5.3, and AFDD 2-5.4 will not be addressed in this paper. While they are

pertinent to USAF IO doctrine, they do not add anything more than is found in AFDD 2-5 to the larger discussion of the relevance of USAF IO doctrine.

AFDD 1, *Air Force Basic Doctrine,* was released in September 1997. From the very beginning AFDD 1 reflects the discussions that led to the inclusion of IW in USAF thought. General Fogleman discussed the fifth dimension of the information realm. AFDD 1 states "warfare is normally associated with the different mediums of air, land, sea, and space. In addition, information is now considered another medium in which some aspects of warfare can be conducted" (AFDD 1 1997, 7). The "fifth realm" has become an accepted airpower principle. AFDD 1 goes on to tie IW activities into the airman's view of the principles of war. The USAF accepts the principles of war familiar to all members of the military: unity of command, objective, offensive, mass, maneuver, economy of force, security, surprise, and simplicity. Under USAF doctrine, IW enables many of these principles to be achieved at a reduced cost in casualties and resources. Mass can be redefined by leveraging the IW characteristics of stealth, precision, and speed to attack critical targets (AFDD 1 1997, 16). Economy of force is enhanced by the dominant battlespace awareness enabled by IO. Security takes on a whole new facet in a world dominated by information technologies. Information plays a central role in every conflict. Security of friendly information resources and denying the adversary the same are critical to the conduct of USAF operations (AFDD 1 1997, 20). Surprise and shock can be achieved with air and space power due to the dominant battlefield awareness provided by air- and space-based intelligence, surveillance and reconnaissance (ISR) assets. While the principles of war do not change, IW offers new ways to achieve the desired effects.

The USAF defines six core competencies. Core competencies are not doctrine, but "they enable the translation of doctrine into operational concepts" (AFDD 1 1997, 27). USAF core competencies are air and space superiority, precision engagement, information superiority, global attack, rapid global mobility, and agile combat support. Information superiority is defined as "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions" (AFDD 1 1997, 31). This definition captures the concepts of IW and IIW. Information superiority is a core competency that allows the USAF to succeed in all of the rest of its core competencies. The USAF needs to dominate the information realm through its ISR capability, to protect its information systems, and to influence the adversary's decision cycle in order to achieve the operational results the country depends on the USAF to provide.

IO are acknowledged as a key element of the capability that the USAF brings to the nation, the joint force commander and coalition forces. AFDD 1 defines information operations as "actions taken to gain, exploit, defend, or attack information and information systems" (AFDD 1 1997, 44). This definition of IO more closely reflects the joint definition of IO than the definition proposed in *Cornerstones*. From discussion to doctrine, IO subsumed IW in parallel to the joint definitions. The AFDD 1 definition is more operational than strategic reflecting the services role as a component of a joint force. USAF doctrine foresees operations in the air, space, and information realms as essential to integrate the application of air and space power to project global strategic military power.

AFDD 1 suggests ways in which IO can be applied to achieve effects generally considered in the purview of more conventional USAF weapon systems. Interdiction missions usually involve aircraft destroying infrastructure targets. It may be possible to achieve the same effects by intercepting or disrupting information flow or by damaging key software or hardware (AFDD 1 1997, 49). Strategic attack can also be carried out in the information realm. C2 is a potential IW target of particular interest in the strategic attack function (AFDD 1 1997, 52). In line with ideas expressed in *Cornerstones*, C2 is a separate function of air and space power

Under AFDD 1 counterinformation is now a function of air and space power. This reflects changes to the roles and missions of the USAF found in *Cornerstones*. Identifying counterinformation as a function of air and space power enables the operationalization of IO in the USAF. Under counterinformation there are both offensive and defensive elements. Offensive counterinformation "destroys, degrades, or limits enemy information capabilities and are dependent on having an understanding of an adversary's information capabilities" (AFDD 1 1997, 53). Defensive counterinformation seeks to protect friendly information, information systems, and IO from adversary IO through OPSEC, COMSEC, COMPUSEC, and counterintelligence. These thoughts can be traced directly to discussions held in the years prior to AFDD 1 publication.

AFDD 2, *Organization and Employment of Aerospace Power*, 28 September 1998, expands upon the ideas found in AFDD 1. AFDD 2 is more of an operational level document than AFDD 1. AFDD 2 stresses the asymmetric value of air and space power when employed in parallel physical attacks against surface forces and information attacks against an adversary's C2 (AFDD 2 1998, 7). AFDD 2, for the first time in USAF

doctrine, spells out the difference between IIW and IW. IIW revolves around surveillance and reconnaissance that "provide the information required to formulate strategy, develop plans, and conduct operations." IW involves activities like "psychological operations (PSYOP), military deception, electronic combat, both physical and information (cyber) attack, and a variety of defensive activities and programs" (AFDD 2 1998, 22). One of the ideas that distinguished USAF discussion on IW from that of other services and the community at large was the distinction between IW and IIW. This distinction was institutionalized in AFDD 2.

AFDD 2 spreads operational responsibility for conducting IO among the various staff elements of the Commander, Air Force (COMAFFOR) or the Joint Force Air Component Commander (JFACC). The COMAFFOR will normally be designated the JFACC when an operation is conducted under a Joint Force Commander (JFC). The JFACC is given specific responsibility for conducting counterinformation operations in support of the JFC's objectives (AFDD 2 1998, 49). The A-3/5 or J-3/5, Operations and Plans, staff element is responsible for coordinating IW, and advising the COMAFFOR/JFACC on available information resources or any information resource organizations supported or supporting the JFC (AFDD 2 1998, 55). The A-6 or J-6, Communications and Information, staff element is responsible for coordinating information protection requirements and procedures with the air operations center (AOC) IW team (AFDD 2 1998, 57). These staff elements are separate from the organizations found in the AOC or joint AOC (JAOC).

The AOC/JAOC will include a specialty team responsible for IW. This team will be comprised of members from a variety of specialties related to IW. A single team

leader will supervise the team members, but they will integrate with the standing teams in the AOC/JAOC (AFDD 2 1998, 73). The standing teams are the strategy division, combat plans division, combat operations division, and the air mobility division. By spreading the IW team members throughout the core teams, the IW team can ensure IO are integrated and coordinated across combat operations. The strategy division does long range planning. For IO the division is responsible for providing JFACC inputs to the JFC for development of the ISR and IO plan. Combat Plans generates and disseminates the orders that provide for the effective employment of airpower in the area of operations. Combat operations division provides feedback to the IW team on the effectiveness of IO based upon the results of ISR reports (AFDD 2 1998, 71). AFDD 2 does not specify the USAF specialties that will make up the IW team. The team has taken over the role formerly performed by the electronic combat cell. AFDD 2-5 goes into more detail on implementing IO.

AFDD 2-5, *Information Operations,* was published 5 August 1998. AFDD 2-5 provides the details on applying IO in USAF operations. Information superiority is characterized as an enabling function achieved through IO. Information superiority is defined as "the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition" (AFDD 2-5 1998, 1). As already noted, information superiority is achieved through IO which is defined as "those actions taken to gain, exploit, defend, or attack information and information systems and include both information-in-warfare and information warfare and are conducted throughout all phases of an operation and across the range of military operations" (AFDD 2-5 1998, 1). IIW is more finely defined in AFDD 2-5 as "the Air

Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities." IW is defined as "information operations conducted to defend the USAF's own information and information systems or conducted to attack and effect an adversary's information and information systems" (AFDD 2-5 1998, 2). All of these definitions build upon and refine the concepts presented in AFDD 1 and AFDD 2.

AFDD 2-5 focuses IO efforts by identifying several considerations central to IO in USAF operations. IIW and IW are separate and distinct functions, but they must be integrated to achieve information superiority. Counterinformation operations must be performed in parallel to exploit the asymmetric advantage provided by IO. USAF IO operations occur at all levels of military conflict and in all phases. The USAF will be prepared to support national, strategic IO. Defensive counterinformation will remain the USAF's priority for the foreseeable future. IW will be implemented through the warfighting commands, not as a separate, stovepiped function. It is possible to develop a campaign plan that is primarily IW, but it is not possible to develop an IW plan separate from an overall campaign plan (AFDD 2-5 1998, 7). These considerations provide combatant commanders, the USAF, and sister services, with a blueprint on how USAF IO operations will be focused, where effort will be expended to improve USAF operations in the short term, and how the USAF sees IO in terms of the overall USAF mission. Counterinformation is the priority and defensive counterinformation is the priority within that function.

Counterinformation is defined as "an aerospace function that establishes information superiority by neutralizing or influencing adversary information activities to varying degrees, depending on the situation" (AFDD 2-5 1998, 9). This definition is actually a step back from the definition provided in AFDD 1. AFDD 1 is fairly unequivocal in asserting that counterinformation will give the US "control" of the information realm. The definition in the glossary of AFDD 2-5 provides yet another definition of counterinformation. The glossary defines counterinformation as actions which "seek to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force" (AFDD 2-5 1998, 40). The glossary definition probably comes closer than any of the others to capturing the essence of counterinformation provided in the explanation in the body of AFDD 2-5. Like air superiority, information superiority is not, and does not need to be, absolute. Commanders need information superiority to conduct other operations, but it does not need to be continuous. Using offensive and defensive counterinformation to establish information superiority where and when needed allows the combatant commander to husband resources to achieve the strategic, operational, and tactical effects desired.

Offensive and defensive counterinformation definitions in AFDD 2-5 encompass ideas put forth in *Cornerstones* and AFDD 1. Offensive counterinformation is "actions taken to control the information environment designed to limit, degrade, disrupt, or destroy adversary information capabilities and are dependent on having an understanding of an adversary's information capabilities." Defensive counterinformation is "actions that protect information, information systems, and information operations from any

potential adversary" (AFDD 2-5 1998, 10). The USAF has defined information attack in a unique way under the doctrine of offensive counterinformation.

Information attack is "those activities taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides" (AFDD 2-5 1998, 15). The concept of information attack was conceived to attack the perceptions of the adversary's decision makers without destroying the systems used to process information. Information attack is more than attacking automated systems, it attacks the information processes the adversary relies upon to orient their decision-making.

IO planning and execution must be integrated into normal operations for combatant commanders. AFDD 2-5 identifies three components required to achieve information superiority: effects-based approach, integrated counterinformation planning, and information warfare organizations (AFDD 2-5 1998, 27). Effects can be achieved at the strategic, operational, or tactical levels of war. The national command authorities are generally responsible for strategic IO effects. The combatant commander and/or the COMAFFOR/JFACC are responsible for operational IO effects. USAF or functional component commanders are responsible for tactical IO effects. This distinction fits with the concept forwarded in the discussion section that the USAF would worry about operational and tactical IW and let someone else worry about strategic IW. The distinction can be seen in the organization of IW teams recommended by AFDD 2-5.

AFDD 2 identifies the IW team as a specialty team supporting the standing teams in the AOC. AFDD 2-5 provides details on the makeup of the IW team. The team is integrated into the AOC which allows it to integrate IW planning into the overall

campaign plan. The core of the team comes from the NAF IW office, AFIWC deployed experts on special technical operations and the commander or operations officer from an IW organization. Specialists in all the different areas of IO will augment this team. The organization of the IW team allows the permanent members to tailor the team to the needs of the commander in support of the combatant commander's theater objectives. The team is responsible for ensuring offensive and defensive counterinformation operations are incorporated into the overall air campaign. Additionally, the IW team will nominate targets to the joint force commander for inclusion in the theater campaign plan. Based upon the joint force commander's objectives and the IW team's recommendations, various IW organizations will be tasked to support the air campaign.

USAF IW organizations identified in AFDD 2-5 include the base level Network Control Centers, major command network operations and security centers, and the AFIWC's Air Force Computer Emergency Response Teams (AFDD 2-5 1998, 35). All of these organizations are designed to perform defensive counterinformation operations. AFDD 2-5 also identifies one IW squadron. The reference is to the 609th IWS that, as discussed earlier, no longer exists. There have been some modifications to USAF organizations not identified in AFDD 2-5.

Organization

As previously discussed, the USAF established the first IW dedicated unit in the military. The 609th IWS had a short life span for many reasons, but lack of a coherent doctrine was a contributor. As doctrine has evolved, interest in developing operational level IW organizations has increased. The defensive counterinformation organizations identified in AFDD 2-5 continue to function as part of the larger national and DoD effort

to protect the national and military information infrastructure. The AFIWC mission allows them to augment combat staffs in forming the IW team in the AOC, but does not replace the need for MAJCOMs to have their own core IW team. US Air Forces in Europe (USAFE) seems to have been one of the first to see the value of developing an IW capability. The 32nd Air Operations Squadron has primary responsibility within USAFE for integrating IO into deliberate and crisis action planning. The squadron is also responsible for training and exercise of IO and special information operations (SIO) (US Air Forces in Europe 1997, 7). In 1997, the 32nd Air Operations Group published *Concept of Operations for Information Operations* to guide the integration of IO into USAFE operations. The basic tenets for organization and function found in the USAFE CONOPS reflect the IW team organization and integration into the AOC detailed in AFDD 2-5.

In the last year the USAF has taken several steps to get organized. In the next year information warfare units will be formed at each of the USAF's NAFs. The first was activated at 9th Air Force, Shaw Air Force Base, South Carolina. This organization consists of approximately thirty personnel who will form the core of the AOC IW team and provide interface with IW organizations in the US during a conflict (Wall 1999, 102). An IW unit will be formed at Air Mobility Command sometime in the year 2000. The USAF is taking steps to implement a service-wide IW organization that can turn the concepts of USAF IO doctrine into operational reality.

As important as the personnel is the development and sustainment of IO tools. The USAF is making strides in this area also. After decommissioning the F-4G and the EF-111, the USAF was left with only one dedicated electronic combat (EC) aircraft, the

EC-130H Compass Call. Compass Call, a communications jammer, was most effective in conjunction with lethal suppression of enemy air defense (SEAD) and nonlethal SEAD. The US Navy picked up this role with the EA-6B and the F-18C configured to shoot high speed antiradiation missiles (HARM). The USAF got back into the lethal SEAD business in the mid-1990s. The USAF fielded the F-16CJ configured to carry the HARM targeting system (HTS). The USAF is also participating in a DoD-wide analysis of alternatives to select a replacement aircraft for the EA-6B (Fulghum 1999, 28). Operations over Kosovo confirmed the requirement for dedicated EC aircraft in future operations and added impetus to the decision to develop a replacement aircraft now to replace the aging EA-6B. Another fallout from Kosovo was the realization that USAF ISR capabilities are also excessively tasked.

The USAF is currently upgrading and modifying the U-2, RC-135, J-8, and E-3. The EC-130E airborne command, control, and communications aircraft completed an upgrade following the Gulf War. These aircraft will continue to be the backbone of the USAF air-breathing ISR and C2 capability into the foreseeable future. The future in this area looks to be in unmanned aerial vehicles (UAV). In Kosovo UAVs were used to spot targets, provide battle damage assessment, track refugees, monitor the withdrawal of Serbian troops, and provide real-time imagery to allied commanders (Timms 1999, 1). Although fifteen UAVs were lost during the operation, UAVs are significantly cheaper than manned aircraft, and no personnel were placed in jeopardy to gather the information provided. The USAF canceled the Dark Star low observable UAV in the fall of 1998. The USAF is moving forward with the development of the Global Hawk UAV that will be larger, provide an increased payload capability over the currently fielded UAV

systems, and loiter longer than any current ISR capability. Global Hawk will also be able to be reconfigured to carry various ISR and C2 packages tailored to the commander's requirements in a specific theater. Work on capabilities to attack and defend computer networks and automated control systems may also be ongoing. Information on these programs would be classified and is not available to the author. USAF conventional IW capabilities are currently stressed by a high operations tempo. While this problem cannot be fixed in the short term, the USAF is planning for the future of its conventional IW capabilities.

Training

Integrating IW into USAF operations will not occur overnight. To effectively develop the organizations and tactics, techniques, and procedures to make IW the core competency called for in USAF IO doctrine requires training for personnel and exercises to evaluate new procedures. The USAF is taking steps to include IO training at all levels of education and to provide training to personnel tasked to conduct IO.

General Fogleman directed that an introduction to IO be added to the curriculums of the intermediate and senior service schools operated by Air University at Maxwell Air Force Base, Alabama. The curriculum of both these schools now offer lessons on USAF and joint IO doctrine. Additionally, a review of the USAF's formal schools list reveals six IO/IW related courses offered for staff level and senior USAF officers. These courses replaced similar introductory and advanced staff courses on EC. The 39th Information Operations Squadron, Hurlburt Field, Florida, has also been tasked to develop an IO introductory course to train the NAF IW flight personnel (39th IOS, 2000). The first course began in November 1999. The course is sixty-nine days long and is designed to

train NAF IW personnel how to integrate IW into plans and exercises and how to integrate into the AOC staff during times of conflict. The 39th is also assisting in the development of an Air Force Tactics, Techniques, and Procedures (AFTTP) manual for IW. AFTTP standardize operations down to the tactical level for USAF personnel. Finally, the 39th is attempting to get a special experience identifier attached to personnel codes for personnel who receive training in IO.

IW exercises have generally been dedicated to testing the robustness of base level network defense. A Green Flag exercise has been held annually at Nellis Air Force Base, Nevada, since the late 1980's to exercise the USAF's EC components. Most Red Flag exercises include EC, ISR, and C2 aircraft. In 1998 the USAF began the Experiment in Expeditionary Force (EFX) exercises. While not specifically targeted at exercising IW forces, EFXs, which are now joint (JEFX), are designed to exercise innovative ideas for projecting USAF combat force more effectively and efficiently. The scenario for the exercise calls for the forward deployment of combat forces without the large planning, intelligence, and operations staffs currently required. The exercise evaluates new ideas for reducing the USAF operational footprint without impeding combat operations (McMichael 2000, 46). The EFX charter is to evaluate experiments proposed by various battlelabs and centers to pick those with the most potential for further development.

In JEFX 99 some 4,000 personnel deployed to ten separate locations were commanded by a combined aerospace operations center at Hurlburt Field, Florida (McMichael 2000, 46). The deputy for this year's exercise was a German air force general connected to the exercise from Ramstein Air Force Base, Germany. In this year's scenario, attacking aircraft were diverted from their planned targets and retasked and

retargeted while airborne. Additionally, the USAF's next generation battle management system, the Theater Battle Management Core System (TBMCS), was run through its paces early in its development so fixes can be integrated early and operations personnel can become familiar with the capability before it is fully fielded. Space- and cyber-based systems are also starting to be exercised.

The Air Force Space Operations Center out of Schriever Air Force Base, Colorado, and a group from Kelly Air Force Base, Texas, are developing aggressor squadrons to exercise space- and cyber-based systems ability to deter IW attacks or survive them if they occur (Diedrich 2000). The space aggressor squadron will eventually be capable of demonstrating counterspace techniques to operators of the USAF space-based assets. In the near term, they have been making use of available technology to demonstrate current vulnerabilities. While not a mature program, the USAF is taking steps to exercise all aspects of IO.

Summary

DESERT STORM initiated a debate amongst military theorists in all of the services over the future of military operations. In the USAF, two major lessons were learned. The first, not addressed in this paper, was that airpower is a decisive form of warfare. The performance of coalition airpower confirmed that technology had finally caught up with theory. The second lesson was that information was critical to the effective and efficient application of airpower. The debate in the USAF led to discussions on how to leverage information technologies as a tool in warfare and then to a distinction between IIW and IW. These concepts were formally recognized in *Cornerstones of Information Warfare* when it was published in 1995. The ideas

presented in *Cornerstones* were modified, updated, and incorporated into USAF doctrine through the AFDDs discussed in this chapter. The development of doctrine led to changes in organization and training to implement the concepts now institutionalized in doctrine.

Chapter 4 will evaluate USAF IO doctrine against joint doctrine and concepts proposed in wider discussions of IO. The purpose of this is to evaluate the relevancy of USAF IO doctrine in today's information environment.

CHAPTER 4

ANALYSIS

> War's political nature and the physical stress and agony of combat will outlive our attempts through technological progress and our most fervent desires to make it bloodless and devoid of violence. (AFDD 1 1997, 6)

Relevancy is a subjective measure that means different things to different people. Before specifically addressing whether USAF IO doctrine is relevant to accomplishing the USAF mission, it is necessary to look at the strengths and weaknesses of USAF IO doctrine. Strengths and weaknesses will be evaluated against joint doctrine and the review of IO thought presented in chapter 2. Training and organization derive from doctrine. For this reason, the analysis of the relevancy of USAF training and organization will flow from the conclusions drawn on the strengths and weaknesses of USAF IO doctrine. The discussion on strengths and weaknesses will also provide background for answering the primary thesis research question: Is USAF IO doctrine, organization, and training relevant in today's IO environment? In order to adequately analyze the answer to this question, it is necessary to provide as objective a definition of relevancy as possible. It is also necessary to define the elements that constitute the current IO environment. The relevancy definition and IO environment will provide the framework upon which to evaluate the USAF's efforts in developing IO doctrine and the training and organization to implement the doctrine.

While USAF IO doctrine might capture the essential elements of IO, it may not be relevant given the environment in which the doctrine must be used operationally. In

order to provide a common measure for analysis, relevancy in this paper is defined by four key questions:

1. Is the doctrine forward looking?
2. Does the doctrine capture the essence of existing thought?
3. Is the doctrine convertible from theory to operations?
4. Does the doctrine accomplish what it is intended to accomplish?

These questions will be measured on a scale of adequate or not adequate. For the purposes of this analysis, adequacy is defined as suitable given the existing environment, capabilities and resources. The relevancy of training and organization will be evaluated with respect to USAF doctrine.

The current IO environment is subject to various interpretations. For the purposes of analysis, the environment will be defined by current political, economic, threat, technology, and non-IO doctrine conditions. Each of these conditions will be briefly described below.

Political: Policy decisions have resulted in a decrease in personnel and equipment and a concurrent increase in commitments to overseas operations. Different numbers are quoted by different sources, but the underlying condition has resulted in an increased operations tempo for US forces in a wide variety of missions.

Economic: The economy is largely driven by the information technologies that make IO possible. The US economy is currently experiencing a record period of growth. This growth has resulted in increased tax receipts for the federal government. An increase in DoD budgets is foreseen as a result of this surplus, but aging equipment and retention issues will continue pressure to reduce force size for the foreseeable future.

Threat: The Gulf War taught nations around the globe a simple lesson. The US fields the most capable military force in the world. The reaction to this lesson is an increase in asymmetric threats to the US. Several nations are developing capabilities to attack US interests using asymmetric approaches made possible by current information technologies.

Technology: As discussed earlier, it only takes 18 months for computers to reach obsolescence. This reflects an environment in which new technologies are occurring more rapidly than the military can respond with potential counters. It appears this trend will continue for the foreseeable future.

Non-IO doctrine: All of the services are attempting to adjust to reduced forces and changing missions by adjusting doctrine. For IO to be truly effective, non-IO doctrine must leverage the capabilities of IO to make combat operations more effective. This effort is in its infancy.

Conclusions on the relevancy of USAF IO doctrine will ultimately be a subjective judgment influenced by the author's experiences and perceptions. The proposed framework provides a glimpse into the considerations used to evaluate USAF IO doctrine. Ultimately, service doctrine is a consensus of theories and ideas derived from experience and perceptions and, hopefully, tested as rigorously as possible.

Comparison

All DoD agencies are moving forward with concepts of IO. The USAF has taken concrete steps to operationalize IO. Compared to the efforts of the joint community, the larger IO, community and foreign nations, USAF efforts have demonstrated strength in some areas and weaknesses in others.

USAF doctrine largely follows the lead of joint doctrine. It is, however, more operationally and tactically focused. USAF doctrine, organization, and training stress the importance of IO to all other operations. According to joint doctrine, IO are "actions taken to affect adversary information systems while defending one's own information and information systems" (Joint Chiefs of Staff 1998, GL-7). AFDD 1 defines information operations as "actions taken to gain, exploit, defend, or attack information and information systems" (AFDD 1 1997, 44). The USAF definition captures not only the defensive and offensive aspects of IO; it also reflects the USAF's focus on collecting and disseminating information. One of the strengths of the USAF definition is the use of terms familiar to airpower operations. The definition of IO contains the same elements used to define doctrine for air and space operations. The use of the terms "gain, exploit, defend or attack" reflects the USAF's focus on the operational and tactical application of IO. The use of terms familiar to airpower operations will facilitate the operationalization of IO.

Organizationally, joint doctrine places responsibility for conducting IO on the JFC. In line with this, USAF doctrine assigns theater responsibility for USAF IO support to the JFC on the Commander, Air Force (COMAFFOR). To facilitate the COMAFFOR's ability to carry out his duties, the USAF is developing IW units at each of the USAF's Numbered Air Forces (NAFs). The NAF commander is usually designated COMAFFOR for one of the geographic or functional combatant commanders. The first of these NAF IW units was activated at 9th Air Force, Shaw Air Force Base, South Carolina (Wall 1999, 102). This organization consists of approximately thirty personnel who will form the core of the air operations center IW team and provide interface with

IW organizations in the United States during a conflict. These organizations will provide the COMAFFOR with knowledgeable, professional information operators.

The effort to build a pool of professional information operators reflects a trend in both US and foreign militaries. The US Army is developing a functional area (FA) specialty for IO. FA 30 officers will coordinate, plan, and integrate IO in support of the commander's campaign plan (US Army 2000). FA 30 officers will be pulled from all branches of the US Army, not just the traditional IO fields. This will bring a wider experience base to the development of US Army IO doctrine in the future. China and Russia are taking steps to increase the professional stature of their information operators. Official Chinese military publications indicate they are contemplating a separate information force (Gertz 1999). The Russians, for their part, raised their radio electronic combat forces to special weapons status; they are no longer considered support troops for the other operational forces (Dick 1993, 390).

The USAF definition of information superiority is another attempt to operationalize IO doctrine. The USAF identifies information superiority as one of the USAF's core competencies. It is on par with air and space superiority in USAF doctrine. The ultimate goal of IO, in joint doctrine, is to achieve information superiority (Joint Chiefs of Staff 1998, I-2). Under both joint and USAF doctrine, information superiority facilitates all other operations. Chinese doctrine indicates that information superiority has eclipsed air superiority in importance for shaping the battlespace in future wars. The Chinese think information superiority provides the opportunity to achieve a strategic advantage without physical conflict (Thomas 1998). Like the USAF, Russia places gaining "electronic superiority" on par with air superiority (Dick 1993, 390). Both

conditions are required to achieve the necessary strategic advantage in twenty-first century conflict. Like the USAF definition of IO, information superiority is defined in terms common to the definitions of air and space superiority. This familiar reference will allow USAF operators to more rapidly understand the concepts and will provide a platform for the development of the follow on tactics and procedures needed to operationalize IO.

USAF IO doctrine establishes counterinformation as the aerospace function that establishes information superiority. Counterinformation is similar to the offensive and defensive IO concepts in joint doctrine. Counterinformation can be either offensive or defensive. By identifying counterinformation as a specific aerospace function, the USAF has provided focus for the operational commanders. Operational commanders understand counterair missions. Counterinformation has been developed along a similar framework to provide a common architecture with other aerospace functions. This commonality will improve the chances of IO being effectively incorporated into USAF operations. It will also allow a broader group of USAF members to understand and apply IO.

The concepts of IW and information-in-war (IIW) are another USAF contribution to the development of IO doctrine. The significance of these two terms lies in the distinction between information tools that facilitate conventional operations and information tools that can be used as weapons to shape an adversary's perceptions. IIW is defined in AFDD 2-5 as "the Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and

dissemination activities; and its global navigation and positioning, weather, and communications capabilities." IW is defined as "information operations conducted to defend the USAF's own information and information systems or conducted to attack and effect an adversary's information and information systems" (AFDD 2-5 1998, 2). In the often-confused world of IO terminology, the USAF's clear distinction between IIW and IW is refreshing. By establishing this distinction, it is easier to understand the offensive characteristics of counterinformation. Too many people get bogged down in the supporting functions (ISR, information collection and dissemination, navigation and positioning, weather, and communications) that are critical to operating a smaller military force structure in a time of increased commitments. The ability of IW to help shape the battlefield for the JFC is also critical. As a new tool, IW is often misunderstood. The joint definition of IW does not make this same distinction. Effectively, the USAF doctrine narrows the definition of IW. This narrow definition enables the operational commanders to separate responsibilities between supporting functions and operational functions.

Chinese and Russian IW doctrine are similar to USAF doctrine. Chinese IW doctrine distinguishes between IW and IIW. They believe the application of information, as a tool of war will make weapons of soft destruction more important than weapons of hard destruction. Chinese doctrine postulates that information-in-war will allow traditional combat tools to be more effective by providing the rapid command and control and accurate targeting information required to survive the rapid pace of the modern battlefield (Thomas 1998). The Russians also distinguish between IW and IIW. Their reconnaissance strike complex provided the genesis of the USAF's IIW concepts. While

there is no officially accepted Russian definition, IW is seen as a way to manipulate adversary perceptions, to protect friendly information, and to target an adversary's information systems (Thomas 1998).

A shortfall in USAF doctrine is the continued use of multiple definitions for each term. Information superiority provides the best example. AFDD 1, published in 1997, defines information superiority as "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions" (AFDD 1 1997, 31). AFDD 2-5, published in 1998, defines information superiority as "the degree of dominance that allows friendly forces the ability to collect, control, exploit, and defend information without effective opposition" (AFDD 2-5 1998, 1). The original definition more fully explains the concept. The AFDD 2-5 definition does a better job of operationalizing the concept. While it might seem like a small thing, the same situation exists with any number of joint definitions. Experts in IO employ terms like dominant battle space knowledge, netwar, and softwar. To the extent that many of these words designate early theories on various branches of IO, they are useful. As IO becomes incorporated into the services doctrine, the terminology needs to be standardized within the services and across the services. In the back of the AFDD booklets, the glossary provides both the joint and the USAF definition of various terms. It is almost as if the authors are providing a decoder ring. If USAF doctrine writers are not satisfied with joint definitions, they should work to get the definitions changed. It does not serve the entire field of IO for each service to develop its own set of terminology. IO, of all the areas of warfare, requires common terminology so

that the various organizations can bring together their individual capabilities to develop a meaningful IO strategy in support of the JFC.

USAF IO doctrine is focused on operational and tactical applications. The doctrine needs more emphasis on the concept of perception management. Like joint doctrine, USAF IO doctrine recognizes that the adversary's decision makers and decision processes are the appropriate targets of an IO campaign. USAF IO doctrine is weak on details about how airpower will affect the message at the strategic level. Even when discussing support operations critical to IO, USAF IO doctrine does not focus at the strategic level. Intelligence support is identified as a critical element in the conduct of IO (AFDD 2-5 1998, 21). The tasks described, however, concentrate on the use of IO tools at the tactical level. No mention is even made of analyzing the decision makers or the cultural influences that can be manipulated to manage their decisions.

Previously, the author proposed definitions for IO and IW. According to the author, IO are actions by military and other governmental agencies to achieve strategic objectives in conflict and peace by protecting friendly use of the information environment and exploiting the information environment in order to shape an adversary's perceptions. The author defines IW as actions taken during time of crisis or conflict to attack information systems directly as a means to alter adversary knowledge or beliefs to achieve or promote specific objectives over a specific adversary or adversaries. USAF IO doctrine's focus on operational and tactical functions is appropriate for its role as a component of a JFC staff. It is not appropriate at the service level as decisions are made on how and where to spend limited dollars to improve the USAF's IO capability. The proposed definitions provide that broader outlook. USAF organization and training need

to be directed to the more strategic concepts behind IO. As a service the USAF understands the tactical application of IW tools. The USAF needs to begin building its understanding of the strategic nature of IO so as to be able to bring the strategic and tactical together in a meaningful operational IO plan.

Both the Chinese and the Russians have grasped the strategic nature of IO. Official Chinese publications encourage civilian and military theorists to develop asymmetrical thinking to enable China to surpass the US as the leader in IW doctrine development (Thomas 1998). The Russians are concentrating their efforts on perception management and reflexive control. They recognize the importance of the human element in decision making and are, therefore, concentrating on unique ways to target decision makers.

The USAF has been at the forefront of exercising IO. The USAF began the Experiment in Expeditionary Force (EFX) exercises to experiment with new IIW tools that would allow the USAF to be more effective in operations. These exercises are now joint. The inclusion of sister services in the exercises should provide a more strategic nature to the exercises. A more strategic IO focus will allow the USAF to leverage the work on IIW capabilities to ultimately improve its IW capabilities.

Like the joint community and the sister services, the USAF is putting a lot of emphasis on attacking and defending networks. To further the ability of USAF network administrators to defend their networks from attack, the USAF is developing aggressor squadrons to exercise the ability of space and cyber based systems ability to deter IW attacks or survive them if they occur (Diedrich 2000). The space aggressor squadron will eventually be capable of demonstrating counterspace techniques to operators of the

USAF space-based assets. In the near term, they have been making use of available technology to demonstrate current vulnerabilities. While not a mature program, the USAF is taking steps to exercise all aspects of IO.

The Chinese and Russians also appear to be exercising their IO capabilities. The Chinese have also begun exercising their IIW tools, and, possibly, their IW tools. In October 1998, for the first time, they tested their ability to integrate several of their military districts (Thomas 1998). On the IW front, China is reported to have launched numerous cyber attacks against Taiwan and the US (Christenson 1999). There are also reports of the Russians participating in sophisticated attacks against unclassified DoD computer networks (Vistica 1999, 52). While the evidence is not conclusive, it does indicate increased use of IO by both the Chinese and Russian governments.

Joint policy requires all joint and service schools to teach IO (Joint Chiefs of Staff 1998, I-5). The USAF has established the 39th Information Operations Squadron to provide common IO training for the service (39th IOS 2000). As discussed earlier, the more common the understanding of IO concepts, the more likely the larger USAF will be able operationalize IO. USAF professional military education (PME) courses at all levels offer training in IO. The inclusion of IO at all levels of PME will eventually payoff. Unfortunately, the current confusion of terms and theories will result in continued misunderstandings by operational forces.

USAF IO doctrine does a good job of focusing IO efforts at the tactical and operational level. The doctrine needs to be adjusted to reflect the strategic nature of IO. USAF IO doctrine also needs to reduce confusion over terms and concepts. The current abundance of terms can only lead to continued confusion about what IO offers to the

warfighter. The clear division of IW and IIW in USAF IO doctrine is one of the few areas where terms not found in joint doctrine help to clarify the field of IO. By focusing discussion in two areas, the concepts allow the service to concentrate effort. Operational commanders understand the offensive ideas behind IW. Supporting commanders can concentrate on the IIW capabilities needed to allow the combatant commander to take advantage of information superiority once it is achieved. The USAF is taking small steps in organization and training to improve its ability to conduct IO.

The NAF IW units will provide a core of professional, experienced information operators. While there will be growing pains, the NAF commander will require these personnel in order to employ airpower effectively in support of the JFC's campaign plan. Training IW unit personnel will be problematic until suitable simulations can be developed to allow the effects of IW to be measured in exercises. EFX experiments will provide the IIW capabilities necessary to the conduct of airpower operations in coming years. Future capabilities to exercise the network and space capabilities will improve the USAF's ability to protect critical IIW capabilities. PME training needs to be focused on doctrinal concepts in order to bring some commonality of terms and concepts to the operational forces. While promising, these organizational and training initiatives pale in comparison to the changes the Chinese and Russians are contemplating.

Is it relevant?

USAF IO doctrine is forward looking. The reduced size of the force and the increased operations tempo are forcing the USAF to look for more efficient means of projecting force. The reduced number of active overseas bases exasperates these political factors. The USAF has had the tools necessary to achieve increased efficiency for years.

Global positioning systems; command and control platforms; intelligence, surveillance and reconnaissance systems (ISR); precision guided munitions; and a host of other systems have been available in varying quantities since before the Gulf War. What the service lacked was an integrating strategy for using these tools. The USAF's IO doctrine provides the strategy.

The most important element of USAF IO doctrine is the distinction between IIW and IW. By separating these two critical aspects of IO, the USAF is able to focus and prioritize system acquisition and tactics development. IIW is at the heart of the USAF originated EFX experiments. This decade-long effort will enable the USAF to continue to support JFC tasking while reducing the number of personnel required to deploy. With the inclusion of sister services and coalition partners, the EFX program promises improvements in IIW at all levels of conflict.

Work on IIW will help to keep the USAF ahead of the many elements of the IO environment, but it simultaneously creates significant vulnerabilities. By separating IW from IIW, operational commanders can concentrate their efforts on protecting friendly information systems and attacking adversary systems. The development of IO doctrine and systems by the Chinese and Russians requires the USAF to concentrate on how best to leverage its technological advantage in moving, processing, and formatting information into a comprehensive strategy to counter potential adversaries with an asymmetric strategy. The operational commanders are the best people to focus these efforts.

Each theater presents different problems that require tailored applications of USAF IO doctrine. The NAF commander is responsible for developing the tailored

concepts for meeting the combatant commander's objectives at all levels of conflict. The development of NAF IW units will eventually provide a core of professional experienced information operators. Unfortunately, confusion in service doctrine, terminology, and training will militate against the success of these units. The USAF must work with its sister services and other DoD agencies to standardize doctrine, terminology, and training. The USAF must expand its doctrine to include more strategic thought. USAF doctrine almost completely ignores the strategic nature of IO. While this makes its IW doctrine more focused, it will also prevent the USAF from contributing to the development of more effective strategic IO plans.

USAF IO doctrine is adequately forward looking. Given the constraints of the current IO environment, the USAF is making gains in operationalizing IO doctrine by adjusting organization and training to include more IO. If this trend continues, current IO doctrine will evolve into a useful tool in the operational commander's kit bag.

USAF IO doctrine fails to recognize the strategic nature of IO. In the verbiage, USAF IO doctrine acknowledges the importance of targeting an adversary's decision makers and decision processes. The doctrine does not, however, follow this acknowledgement with any concrete thought on how to employ IO to influence the adversary's decision makers. USAF IO doctrine tends to concentrate on methods for influencing the adversary's information tools and decision processes. This is true in the way supporting operations are described as well. Intelligence plays a critical role in the development of an effective IO plan. USAF IO doctrine does not direct intelligence support to collect information on decision makers or the cultural influences that effect their decisions. Current thought on IO stresses the necessity of evaluating the cultural,

political and personal outlook of an adversary's leaders in order to develop an IO strategy that will achieve the overall campaign objectives. USAF IO doctrine is useful in developing the operational level application of IO. It needs to expand to include more thought on perception management as an important aspect of IO.

USAF IO doctrine is not adequate in the current IO environment. Potential adversaries are concentrating their efforts on developing asymmetric tactics. USAF IO doctrine reflects a more symmetric approach to warfare. The doctrine is tied to the development of technologies without enough emphasis on the human element. If USAF doctrine does not expand to include more emphasis on effecting decision makers, the USAF will not be able to participate as fully in the development of strategic IO plans as our sister services and even some potential coalition partners.

USAF IO doctrine is only partly convertible from theory to operations. To the extent that USAF IO doctrine captures the operational and tactical application of IW, it provides a clear road map for operational commanders. Without the strategic piece, however, USAF IO doctrine seems to advocate IO for the sake of IO. IO must be part of a larger campaign plan to achieve strategic objectives. IO must integrate all of the elements of a nation's power (diplomatic, economic, information, and military) to be truly effective. The USAF, as a component, is only directly responsible for application of IO at the operational and tactical levels. USAF IO doctrine, however, must capture the strategy piece of IO if USAF operational commanders are to be able to contribute to the development of a comprehensive IO campaign plan. The USAF brings some powerful air- and space-based systems to the table. If USAF thought does not envision a strategic

application for these systems, then they cannot be properly integrated into the overall IO strategy.

USAF IO doctrine cannot be adequately translated from theory to operations. The demise of the 609th Information Warfare Squadron was a result of a poor understanding of IO. The USAF has not obviously made enormous gains in understanding. The development of the NAF IW units and the 39th Information Operations Squadron are promising steps toward a better understanding of IO. The USAF must stick with these initiatives even though the payoff is not obvious. IO is an emerging doctrine. There will be growing pains as the doctrine evolves from its current emphasis on operational and tactical applications to a more strategic outlook. If the USAF can maintain its commitment to operationalizing IO, its current activities in training and organization will payoff in the future as the entire DoD community achieves a common understanding of IO.

Ultimately it is too early to know if USAF IO doctrine accomplishes the goal set out in the forward of AFDD 2-5 *Information Operations*: "gaining and maintaining information superiority is a critical task for commanders and an important step in executing the remaining Air Force core competencies" (AFDD 2-5 1998, i). IO has the potential to facilitate all other USAF missions. There are positive indicators that USAF training and organization are adjusting to incorporate IO. Air operations in Kosovo provided the first opportunity to demonstrate USAF IO doctrine in combat operations. General Clark, Admiral Ellis, and Lieutenant General Short all acknowledged that IO was not done well at any level of the Kosovo operation (Ellis 1999). While IO will play a role in facilitating USAF operations, IO must be conducted as part of a larger, strategic

campaign plan. Time will tell if USAF combatant commanders can develop airpower plans that truly leverage IO.

USAF IO doctrine is relevant, but not adequate. It is sufficiently forward looking to provide a roadmap for operational commanders. At the operational and tactical levels, USAF IO doctrine captures the essence of current IO thought and is translatable from theory to operations. At the strategic level, however, current USAF IO doctrine is not adequate. In an environment of reduced personnel and increased commitments, the USAF needs to concentrate its efforts on the strategic and asymmetric aspects of IO. While this may require the diversion of funds from more conventional programs, the payoff in the future may be enormous. The threat for the foreseeable future will require the US to counter asymmetric threats from a variety of different adversaries. USAF doctrine does not fully explore ways to use air and space power to counter asymmetric threats. As a component force it is important to fully understand the operational and tactical application of USAF IO tools. As a contributor to the overall IO strategy, it is necessary for USAF personnel to have a better understanding of the strategic aspects of IO.

USAF IO training is relevant, but not adequate. In line with DoD direction, the USAF is developing personnel with IO experience to provide the operational commanders with a core of knowledgeable information operators. The problem with training is not a USAF unique issue. Without a common understanding of IO terms and concepts, it is difficult to evaluate the value of the training. Within the services, the institutional perception of IO seems to mean psychological operations to the US Army, counter network defense and attack to the USAF, and IIW to the US Navy. IO is all of

these things and much more. USAF training needs to lead the way by emphasizing the strategic nature of IO. Command and control exercises need to begin weeks in advance with a requirement for the NAF commander to evaluate the human and cultural aspects of the potential adversary. The NAF IW unit needs to learn what questions to ask the intelligence community. The USAF regularly practices evaluating the integrated air defense systems and the command and control networks. IO, at the strategic level, requires the operational commanders to evaluate the decision makers as well. USAF leadership needs to fight for commonality in terminology. IO is strategic. All the services need to work together to develop the military tools needed to achieve the strategic objectives of the JFC campaign. As we develop these tools, operational commanders and their staffs need to be trained how to use them.

USAF IO organization is also relevant, but not adequate. The NAF IW units are a start. IO organization in the USAF tends to be intelligence centered. The Air Staff agency responsible for IO is part of the intelligence directorate. The operations directorate should be responsible for IO. The Air Intelligence Agency commands the 39th Information Operations Squadron. IO needs to become operations centered. USAF doctrine stresses the operationalization of IO, but the organization reflects the dominance of supporting agencies. DoD has given primary responsibility for IO to SPACECOM. In line with this organizational decision, the USAF should place IO under the Air Force Space Command. Just as the USAF has developed air operations squadrons to support air operation center operations, it should develop information operations squadrons to provide a standing IW cell for the air operations center. These organizations need to be larger than the current NAF IW units. USAF IW units need to be robust enough to

provide personnel for continuous combat operations, training, and, eventually, testing of tactics and procedures. Multiple technical and operational specialties should be represented in the makeup of the IO squadron.

If the USAF hopes to truly operationalize IO, IO squadrons need to be given priority in personnel and resources. At the same time, the USAF needs to resist the temptation to rename current squadrons as IO units just because their current mission can be classified as an IO mission. This temptation reflects the operational and tactical focus of the USAF. IO is strategic. Units preparing to plan and execute IO campaigns need to operate at the strategic/theater level. The existing operational units are tools in a kit bag. Every mission they conduct will not be IO. The personnel will not inherently be IO experts. Renaming the squadrons simply adds credence to the argument that IO is just the current buzzword. Even with today's reduced resources, the USAF can organize better to conduct IO.

Summary

This chapter analyzed the current state of USAF IO doctrine with respect to joint doctrine and the wider field of IO thought. Significant strengths and weaknesses of USAF IO doctrine were identified. Finally, the relevancy and adequacy of USAF IO doctrine was evaluated. Based upon the definitions of relevancy and adequacy proposed, USAF IO doctrine, training, and organization are relevant. The USAF needs to continue to push the envelope in developing doctrine, training, and organizations that incorporate IO into day-to-day operations. Current doctrine, organization, and training provide the bedrock upon which to build a future force to fight emerging asymmetric threats. The USAF needs to fight the urge to let its IO organizations and training simply evolve.

Some revolutionary steps need to be taken in order to truly operationalize IO. The USAF needs to lead the charge in standardizing terms across the DoD. IO is inherently strategic. The USAF cannot develop coherent, successful IO campaign plans, if it is not even able to agree upon standard definitions. To be more credible, the USAF needs to improve its doctrine with respect to the strategic aspects of IO.

Chapter 5 will provide conclusions for the thesis based upon the analysis in this chapter and the background information from the previous chapters. Chapter 5 will also make recommendations for further research in this area.

CHAPTER 5

CONCLUSIONS AND RECOMMENDATIONS

> Thus, those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations. (Sun Tzu, 79)

Conclusions

This research project was conducted to evaluate the relevancy of the USAF's IO doctrine, training, and organization. The analysis evaluated how the USAF's doctrine and organization comply with JCS guidance on IO. It also looked at some concepts proposed by other writers for their applicability to USAF IO doctrine. The focus of the thesis was the adequacy of the USAF's IO doctrine, training, and organization.

As the USAF begins to posture to conduct operations in the twenty-first century, it needs to be prepared to subdue US adversaries without battle. IO provide the asymmetric edge the US military needs to counter the growing threat of cyberwarfare, weapons of mass destruction, and terrorism we can expect in the early part of this next century. The USAF must expand its capability to defend its own information and information systems while simultaneously developing airpower tools that contribute to the JFC theater IO objectives.

USAF IO doctrine, training, and organization are relevant, but not adequate to enable the USAF to have a substantial impact at the strategic level. The USAF needs to continue to push the envelope in developing doctrine, training, and organizations that incorporate IO into day-to-day operations. Current USAF doctrine, organization, and training provide the bedrock upon which to build a future force to fight emerging

asymmetric threats. The USAF needs to fight the urge to let its IO organizations and training evolve. Some revolutionary steps need to be taken in order to truly operationalize IO. The USAF needs to lead the charge in standardizing terms across the DoD. IO is inherently strategic. The USAF cannot develop coherent, successful IO campaign plans if it is not even able to agree upon standard definitions. To be more credible, the USAF needs to improve its doctrine with respect to the strategic aspects of IO.

There is really very little that is new in the field of IO. The revolutionary thing about IO is the emphasis on integrating several disparate fields into a comprehensive campaign in order to manage an adversary's perceptions in a predictable manner. New tools to take advantage of the information technologies that are now available are being added to the more conventional mix of psychological operations, electronic warfare, military deception, physical attack, and OPSEC, COMSEC and COMPUSEC. While these new information tools provide the US military with a significant advantage in the conduct of symmetric and asymmetric operations, they also create a new vulnerability for US operations. It is in this area that the USAF makes the largest contribution to IO doctrine.

By clearly distinguishing between IW and IIW, the USAF enables operational level commanders to more readily grasp the opportunities and pitfalls of IO. The joint definition of IW does not make this same distinction. Effectively, the USAF doctrine narrows the definition of IW. This narrow definition enables the operational commanders to separate responsibilities between supporting functions and operational

functions. In the often-confused world of IO terminology, the USAF's clear distinction between IIW and IW is refreshing.

In his 1996 book *Cyberwar: Security, Strategy, and Conflict in the Information Age*, Alan Campen identifies twenty-one countries that potentially had the capability to conduct IW (Campen 1996, 87). This list contains traditional foes, allies, and third world countries. It did not mention Yugoslavia. Yet, during the recent conflict over Kosovo, Slobodan Milosevic arguably did a better job of both internal and external perception management than NATO. Unfortunately, nationhood and leading edge technology are not required to compete in the information game. Campen's estimate may be well short of the total number of countries able to conduct IW in the year 2000.

As demonstrated in this thesis, Russia and China are aggressively pursuing IO capabilities. While Russia may not have the supporting infrastructure or economy to be a significant short-term threat, the same cannot be said about China. Not only are the Chinese currently threatening military actions over the fate of Taiwan, they are, reportedly, also pursuing the development of an information corps of equal stature to their other service branches. China has the supporting infrastructure and economy to develop the technologies needed to conduct IO. IO is a growing field of interest to militaries around the world. The USAF needs to continue to develop the doctrine, organizations, and training necessary to contribute to the combatant commander's ability to conduct IO.

The development of this thesis was hampered by the fact that IO is an evolving concept. There are some commonly recognized dimensions to IO; however, there are many aspects that are not widely accepted. It is not possible to address all the dimensions

of IO identified in current literature. It was also hampered by the lack of open source information on new equipment and possibly even new organizations. Open source information is difficult to obtain because IO technology is cutting edge. New capabilities in information technology double every one and one-half to three years (Libicki 1994, 7). To stay ahead of this wave requires a massive investment in infrastructure and capability. The sensitivity of this investment induces the military to classify most of the programs directed toward IO.

Recommendations

USAF doctrine is adequate for applying IO at the operational and tactical levels of conflict. Doctrine writers at the USAF's doctrine center need to concentrate their efforts on working with our sister services and the joint staff on building a more robust strategic IO doctrine. The first step in the development of a better IO doctrine for the US military is a common set of terminology. USAF terminology tends to ignore the perception management functions of IO. The concepts of IIW and information attack, however, add to the overall discussion of IO and should be adopted by the joint community. IO is in its infancy. Joint doctrine needs to continue to mature. The USAF can contribute to this process.

Organizationally, the USAF needs to place responsibility for the development of IO tools and training under US Air Force Space Command. This will align USAF organization with the joint community. Space Command will then be responsible for providing the operational commanders, USAF's numbered air forces (NAF), with a core of professional, experienced information operators. The current NAF IW units are a

good first step, but they need to be made large enough to operate as an IW cell without augmentation for a prolonged period of time.

The USAF doctrine of incorporating the IW cell members into the standing organizations in the air operations center needs to continue. During peacetime, the IW units assigned to the NAF will be responsible for training the operational forces through periodic instruction, exercises, and theater specific conferences. This same model has been used successfully with intelligence support of the various theaters. Like intelligence, IO can only be operationalized if it becomes part of normal operations. Professional information operators can only be developed if an infrastructure is developed to encourage the development of their skills and their ideas. New ideas will be necessary to continue the growth of IO doctrine.

At the Pentagon, IO needs to be represented by the same staff that represents fighter and bomber issues on the staff. Like air operations, IO is ultimately the operational commander's responsibility. The higher headquarters' staff should reflect this fact. If USAF doctrine is to be believed, information superiority makes all other operations possible. USAF organization needs to reflect that commitment.

IO training cannot be truly effective until a common set of terms is determined. The establishment of a unit dedicated to training IO is a good first step. The Experiment in Expeditionary Force exercises is another good step. It needs to be broadened to include IW tools as well as IIW tools, but that may not be practical given the current state of technology. Any exercise including the NAF staff needs to incorporate IO. Since IO can be most effective prior to the opening of hostilities, command post exercises need to begin with an IO scenario that requires the operational commander and the IW cell to

interact with higher headquarters' IO cells to develop an IO campaign from the strategic to the tactical level. The initial attempts at this will be problematic, but no progress will be made until operational units begin to exercise IO. Operational commanders will not magically understand and use IO when conflict begins. The USAF needs to put doctrine into practice through its training and exercise program.

Further Research

IO is an emerging field. Potential adversaries and potential coalition partners are working today to define what IO means to them. The entire field is ripe for research. This thesis would have benefited from more research on the development of IO training and the incorporation of IO into exercises. No research information was available at the time of this writing. The 39th Information Operations Squadron began its first training class in November 1999. The Experiment in Expeditionary Force exercise was conducted in August 1999. Detailed results were not available at the time of this writing.

Other areas of potential research include the development of information attack tools. By their nature, many of these tools will be classified. An evaluation of how these tools contribute to overall USAF operations would be of value to USAF and joint doctrine development as well. While the tools under development are probably of value to the USAF, in a time of reduced resources, an evaluation of their utility would not be a wasted effort.

Summary

IO may indeed change the way the world's militaries conduct combat operations in the future. If IO achieve this promise, a true revolution in military affairs will have occurred. At the present time, however, IO are maturing in fits and start. The USAF has

a robust doctrine for conducting IO at the operational and tactical level. In the judgment of the author, USAF doctrine is as good as or better than joint doctrine. USAF and sister service doctrine writers need to develop a better sense of the strategic nature of IO. Once this occurs, the doctrine can be written; new organizations can be developed; and operational forces can be trained to incorporate IO when tasked by the National Command Authorities.

GLOSSARY

Civil Affairs. The activities of a commander that establish, maintain, influence or exploit relations between military forces and civil authorities, both governmental and nongovernmental, and the civilian populace in a friendly, neutral or hostile area of operations in order to facilitate military operations and consolidate operational objectives (Joint Chiefs of Staff 1998, GL-4).

Computer Network Attack (CNA). Operations to disrupt, deny, degrade or destroy information resident in computers and computer networks or the computers and networks themselves (Joint Chiefs of Staff 1998, GL-5).

Counterinformation. Actions which seek to establish a desired degree of control in information functions that permits friendly forces to operate at a given time or place without prohibitive interference by the opposing force (AFDD 2-5 1998, 40).

Cyberspace. That intangible place between computers where information momentarily exists on its route from one end of the global network to the other (Schwartau 1994, 49).

Defensive Counterinformation. Actions which seek to protect friendly information, information systems and IO from adversary IO through OPSEC, COMSEC, COMPUSEC and counterintelligence (AFDD 1 1997, 53).

Defense Information Infrastructure (DII). The shared or interconnected system of computers, communications, data applications, security, people, training and other support structures serving DoD local, national and worldwide information needs (Joint Chiefs of Staff 1998, GL-5).

Defensive Information Operations. The integration and coordination of policies and procedures, operations, personnel and technology to protect and defend information and information systems (Joint Chiefs of Staff 1998, GL-5).

Dominant Battlespace Knowledge. Everything from automated target recognition to knowledge of an opponent's operational scheme and the networks relied on to pursue that scheme. The objective is to create a large gap between US forces and any opponent in awareness and understanding of everything of military significance in any arena in which we may be engaged (Johnson 1996, 4).

Electronic Warfare (EW). Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three major subcategories are electronic attack, electronic protection and electronic warfare support (Joint Chiefs of Staff 1998, GL-6).

Global Information Infrastructure (GII). The worldwide interconnection of communications networks, computers, databases and consumer electronics that make vast amounts of information available to users (Joint Chiefs of Staff 1998, GL-6).

Information Assurance. Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and nonrepudiation (Joint Chiefs of Staff 1998, GL-7).

Information Attack. Those activities taken to manipulate or destroy an adversary's information or information system without necessarily changing visibly the physical entity within which it resides (AFDD 2-5 1998, 15).

Information-in-war (IIW). The Air Force's extensive capabilities to provide global awareness throughout the range of military operations based on its integrated intelligence, surveillance, and reconnaissance (ISR) assets; its information collection and dissemination activities; and its global navigation and positioning, weather, and communications capabilities (AFDD 2-5 1998, 2).

Information Operations (IO). Actions taken to affect adversary information systems while defending one's own information and information systems (Joint Chiefs of Staff 1998, GL-7).

Information Operations. Actions taken to gain, exploit, defend, or attack information and information systems (AFDD 1 1997, 44).

Information Operations. Actions taken in support of political and military objectives which influence decision makers by affecting other's information while exploiting and protecting one's own information (Santee 5 October 1999).

Information Operations. Actions by military and other governmental agencies to achieve strategic objectives in conflict and peace by protecting friendly use of the information environment and exploiting the information environment in order to shape an adversary's perceptions (Author's definition).

Information Superiority. The capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same (Joint Chiefs of Staff 1998, GL-7).

Information Superiority. The ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same and, like air and space superiority, includes gaining control over the information realm and fully exploiting military information functions (AFDD 1 1997, 31).

Information Warfare (IW). Information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries (Joint Chiefs of Staff 1998, GL-7).

Information Warfare. Information operations conducted to defend the Air Force's own information and information systems or conducted to attack and effect an adversary's information and information systems (AFDD 2-5 1998, 2).

Information Warfare. An electronic conflict in which information is a strategic asset worthy of conquest or destruction (Schwartau 1994, 13).

Information Warfare. Actions taken during time of crisis or conflict to attack information systems directly as a means to alter adversary knowledge or beliefs to achieve or promote specific objectives over a specific adversary or adversaries (Author's definition).

INFOSEC. The protection and defense of information and information systems against unauthorized access or modification of information, whether in storage, processing or transit, and against denial of service to authorized users (Joint Chiefs of Staff 1998, GL-7).

Military Deception. Targets adversary decision makers through effects on their intelligence collection, analysis and dissemination systems (Joint Chiefs of Staff 1998, GL-8).

National Information Infrastructure (NII). The nation-wide interconnection of communications networks, computers, databases and consumer electronics that make vast amounts of information available to users (Joint Chiefs of Staff 1998, GL-8).

Netwar. A conflict in which a combatant is organized along networked lines or employs networks for operational control and other communications (Arquilla 1996, vii).

Offensive Counterinformation. Actions that destroy, degrade, or limit enemy information capabilities and are dependent on having an understanding of an adversary's information capabilities (AFDD 1 1997, 53).

Offensive Information Operations. The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect adversary decision makers to achieve or promote specific objectives. These capabilities include operations security, military deception, psychological operations, electronic warfare, physical attack and/or destruction and special information operations (Joint Chiefs of Staff 1998, GL-9).

OPSEC. Slows the adversary's decision cycle and provides the opportunity for easier and quicker attainment of friendly objectives (Joint Chiefs of Staff 1998, GL-9).

PSYOP. Actions to convey selected information and indicators to foreign audiences. They are designed to influence emotions, motives, reasoning and ultimately, the behavior of foreign governments, organizations, groups and individuals (Joint Chiefs of Staff 1998, GL-10).

Public Affairs. Those public information, command information and community relations activities directed toward both the external and internal publics with interest in the Department of Defense (Joint Chiefs of Staff 1998, GL-10).

Reflexive Control. A means or method used to convey specially prepared information to a person, organization or country to influence the adoption of predetermined decision desired by the initiator of the action (Thomas 1999).

Softwar. The hostile use of global television to shape another nations will by changing its vision of reality (de Caro 1997).

Special Information Operations (SIO). Information operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the United States, require a special review and approval process (Joint Chiefs of Staff 1998, GL-10).

Strategic Information Warfare. The battle off the battlefield. The shaping of the political context of the conflict (Stein 1995, 33).

Strategic Information Operations. Those military and governmental operations that protect and exploit the information environment to attain strategic objectives (Kuehl 1997, 32).

REFERENCE LIST

Air Force doctrine document 1: Air Force basic doctrine. 1997. *See* U.S. Air Force. 1997.

Air Force doctrine document 2: Organization and employment of aerospace power. 1998. *See* U.S. Air Force. 1998a.

Air Force doctrine document 2-5: Information operations. 1998. *See* U.S. Air Force. 1998b.

Ahrari, M. Ehsan. 1997. Chinese prove to be attentive students of information warfare. *Jane's Intelligence Review* 9, no. 10 (October): 469-473.

Alberts, David S. 1996. Defensive information warfare. Thesis, National Defense University, Washington, DC.

Aldrich, Richard W. 1996. The international legal implications of information warfare. Thesis, USAF Institute for National Security Studies, US Air Force Academy, Colorado.

Anderson, Christina M., Capt. 1997. Development of a national information warfare strategy: A reengineering approach. Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Arquilla, John, and David Ronfeldt. 1996. *The advent of netwar*. Santa Monica, California: RAND.

Barnette, Roger W. 1998. Information operations, deterrence and the use of force. *NWC Review* (spring). Journal on-line. Available from http://www.nwc.navy.mil/press/review/1998/spring/amt1_sp8.htm. Internet accessed 26 July 1999.

Bass, Carla D. 1998. *Building castles on sand?: Ignoring the riptide of information operations*. Thesis, Air University, Maxwell Air Force Base, Alabama.

Becker, Elizabeth. 1999. Military leaders tell congress of NATO errors in Kosovo. *New York Times*. Newspaper on-line. Available from http://ebird.dtic.mil/Oct1999/e19991015tell.htm. Internet accessed 15 October 1999.

Bouchard, Ronald M., Lt Col (P). 1999. *Information operations in Iraq*. Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Buchan, Glenn. March 1996. Information war and the Air Force: Wave of the future? Current Fad? *RAND Issue Paper*. Santa Monica, California: RAND.

Bunker, Robert J. 1996. Generations, waves and epochs: Modes of warfare and the RPMA. *Airpower Journal* 10, no. 1 (spring): 18-28.

Butler, Bradley L., Col. 1996. The need for a USAF information warfare (IW) Strategy for military operations other than war (MOOTW). Thesis, Air War College, Maxwell Air Force Base, Alabama.

Campen, Alan D., ed. 1992. *The first information war: The story of communications, computers and intelligence systems in the Persian Gulf War*. Fairfax, Virginia: AFCEA International Press.

Campen, Alan D., Douglas H. Dearth, and R. Thomas Goodden. 1996. *Cyberwar: security, strategy, and conflict in the information age*. Fairfax, Virginia: AFCEA International Press.

Chapman, William G. 1997. Organizational concepts for the 'sensor-to-shooter' world: The impact of real-time information on airpower targeting. *Air Command and Staff College, Correspondence Course*. CD ROM. Maxwell Air Force Base, Alabama: Air University, June.

Chizum, David G. 1985. *Soviet radioelectronic combat*. Boulder: Westview Press.

Christenson, Sig. 1999. Pakistani hackers tap Lackland. *San Antonio Express-News*. Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/e19991103lackland.htm. Internet accessed 3 November 1999.

Cornerstones of information warfare. 1995. *See* U. S. Air Force. 1995.

Crystal, Gregory C. 1999. E-mail interview response to several questions posed by Major James L. Griffith, Fort Leavenworth, Kansas, regarding Lt Col Crystal's experiences with information operations while on active duty. 2 November 1999.

Davis, Morman C., Maj. 1997. The Marine Corps and information operations. *Marine Corps Gazette* 81, no. 4: 16-22.

de Arcangelis, Mario. 1985. *Electronic warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts*. Poole: Blandford Press.

de Caro, Chuck. 1997. Softwar. *Air Command and Staff College, Correspondence Course*. CD ROM. Maxwell Air Force Base, Alabama: Air University, June.

Devereux, Tony. 1991. *Messenger Gods of battle: Radio, radar, sonar. The story of electronics in war*. London: Brassey's.

Dick, Charles. 1993. Russia views on future war - part 1. *Jane's Intelligence Review* 5, no. 9 (September 1993): 390-392.

Diedrich, John. 2000. Star wars in cyberspace. *Colorado Springs Gazette*. Newspaper on-line. Available from https://ca.dtic.mil/cgi-bin/ebird?doc_url=/Jan2000/s20000124cyberspace.htm. Internet accessed 24 January 2000.

Drogin, Bob. 1999. U.S. Scurries to erect cyber-defenses. *Los Angeles Times*. Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/e19991101scurries.htm. Internet accessed 1 November 1999.

Dunlap, Charles J., Jr. 1999. *A virtuous warrior in a savage world.* Website. Available from http://www-cgsc.army.mil/dao/Files/LLS%20article%202%20--%GEN%20Schoomaker.htm. Internet accessed 4 August 1999.

Ellis, James, Admiral. 1999. Joint Task Force Noble Anvil Lessons Learned briefing prepared by Admiral Ellis following the completion of Kosovo operations for which he was the joint force commander.

Fadok, David S. 1994. John Boyd and John Warden: Air power's quest for strategic paralysis. Thesis, US Air War College, Maxwell Air Force Base, Alabama.

Fogleman, Ronald L. 1995. Fundamentals of information warfare - An airman's view. Keynote address presented at the National Defense University Foundation Conference on the Global Information Explosion, Washington, D.C. Available from http://www.af.mil/news/speech/current/Fundamentals_of_Information.htm.

Fulghum, David A. 1998. Cyberwar plans trigger intelligence controversy. *Aviation Week & Space Technology* 148, no. 3 (19 January 1998): 52-56.

_____ 1999. USAF sizes up next electronic combat aircraft. *Aviation Week & Space Technology*. Newspaper on-line. Available from http://ebird.dtic.mil/sep1999/s19990921usaf.htm. Internet accessed 21 September 1999.

Garden, Timothy. 1989. *The technology trap: Science and the military*. McLean, Virginia: Brassey's Defence Publishers.

Gertz, Bill. 1999. China plots winning role in cyberspace. *The Washington Times*. Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/e19991117plot.htm. Internet accessed 17 November 1999.

Graham, Bradley. 1999. Military grappling with roles for cyber warfare. *Washington Post.* Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/e19991108grappling.htm. Internet accessed 8 November 1999.

Gray, Jim. 1999. E-mail interview (with follow up questions) response to questions posed by Major James L. Griffith, Fort Leavenworth, Kansas, regarding Col Gray's experiences with information operations while on active duty. E-mail 29 August 1999/25 August 1999.

Griffith, Samuel B. 1963. *Sun Tzu, the art of war*. Oxford: Oxford University Press.

Hill, Peter C.J. 1999. Electronic and information warfare in the digital battlespace. Keynote address presented at the Shephard EW Conference 99, London England.

Hoffman, Bruce. 1994. Responding to terrorism across the technological spectrum. Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Hoffman, Lisa. 1999. U.S. opened cyber-war during Kosovo fight. *Washington Times*. Newspaper on-line. Available from http://ebird.dtic.mil/Oct1999/ e19991025cyber.htm. Internet accessed October 25, 1999.

Hollman, Ryan D., Capt. 1998. A descriptive study of information operations and information warfare awareness in the United States Air Force. Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Howard, Michael, and John F. Guilmartin, Jr. 1994. Two historians in technology and war. Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Huber, Arthur F., Philip S. Sauer, J. Lawrence Hollett, Kenneth Keskel, William L. Shelton, Jr., and John T. Dillaplain. 1996. *The virtual combat air staff: The promise of information technologies*. Santa Monica, California: RAND.

Jablonsky, David. 1994. The owl of minerva flies at twighlight: Doctrinal change and continuity and the revolution in military affairs. Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Jensen, Owen E., Col. 1994. Information warfare: Principles of third-wave war. *Airpower Journal* 8, no. 4. (winter): 35-44.

Johnson, Stuart E., and Martin C. Libicki, eds. 1996. *Dominant battlespace knowledge*. Washington, DC: National Defense University.

Joint Chiefs of Staff. 1998. Joint Publication 3-13: *Joint doctrine for information operations*. Washington, DC: Government Printing Office.

_____. 1996. *Joint Vision 2010*. Washington, DC: Government Printing Office.

Kitfield, James. 1999. Command and Control the Messenger. *National Journal.* Newspaper on-line. Available from http://ebird.dtic.mil/Sep1999/ e19990913commandand.htm. Internet accessed 13 September 1999.

Krepinevich, Andrew F., Jr. 1995. *Missed opportunities: An assessment of the roles and missions commission report.* Washington, DC: Defense Budget Project.

_____. 1996. *The Air Force of 2016.* Washington, DC: Center for Strategic Budgetary Assessments.

_____. 1997. The military-technical revolution: A preliminary assessment. *Air Command and Staff College, Correspondence Course.* CD ROM. Maxwell AFB, Alabama: Air University, June.

Kuehl, Dan Dr. 1997. Defining information warfare. *The Officer* 73, no. 11 (November 1997): 31-33.

Lawlor, Bruce M. 1998. Information Corps: DoD needs to tap the civilian expertise resident in its reserve component. *Armed Forces Journal International.* 135:26-28.

Libicki, Martin C. 1994. *The mesh and the net: Speculations on armed conflict in a time of free silicon.* Washington, DC: National Defense University.

Mahnken, Thomas G. 1995-96. War in the information age. *Joint Forces Quarterly* No. 10 (winter): 39-43.

Mann, Edward, Col. 1994. Desert Storm: The first information war? *Airpower Journal* 8, no. 4 (winter): 4-14.

McGuffee, Robert W. 1999. Information warfare - A new element of the conflict spectrum. Speech presented at the Shephard EW Conference 99, London, England.

McLendon, James W., Col. 1999. Battlefield of the future, Chapter 7. Website. Available from http://www.airpower.Maxwell.af.mil/airchronicles/ battle/chp7.html. Internet accessed 26 July 1999.

McMichael, William H. 2000. Joint experiment in expeditionary force. *Air Force Magazine.* Magazine on-line. Available from http://ca.dtic.mil/cgi-bin/ebird ?doc_url=/Jan2000/s20000107joint.htm. Internet accessed 7 January 2000.

Meader, Gerald H. 1997. Information warfare: Few challenges for public international law. Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Molander, Roger C., Peter A. Wilson, David A. Mussington, and Richard F. Mosic. 1998. *Strategic information warfare rising*. Santa Monica California: RAND.

Munro, Neil. 1991. *The quick and the dead: Electronic combat and modern warfare*. New York: St. Martin's Press.

Morris, Chris, Janet Morris, and Thomas Baines. 1995. Weapons of mass protection: Nonlethality, information warfare and airpower in the age of chaos. *Airpower Journal* 9, no. 1 (spring): 15-29.

Newman, Herb W., Lt Col. 1999. Digital data warfare tools: Should CINCs have control? Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Newman, Richard J. 1999. The New Space Race. *U.S. News & World Report*. Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/e19991101space.htm. Internet accessed 1 November 1999.

Parker, Geoffrey. 1988. *The military revolution: Military innovation and the rise of the West, 1500–1800*. Cambridge: Cambridge University Press.

Pease, Michael R., LCDR. 1998. Information superiority: Where's the beef? Thesis, Naval War College, Newport, Rhode Island.

Santee, Jay Col. E-mail interview response to several questions posed by Major James L. Griffith, Fort Leavenworth, Kansas, regarding Col Santee's experiences with information operations. E-mail 9 September 1999/5 October 1999.

Schechtman, Gregory M., Capt. 1997. Manipulating the OODA loop: The overlooked role of information resource management in information warfare. Thesis, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio.

Schneider, Michael W., Maj. 1994. Electromagnetic spectrum domination. 21st century center of gravity or achilles heel? Monograph, School of Advanced Military Studies, Fort Leavenworth, Kansas.

Schwartau, Winn. 1994. *Information warfare: Chaos on the electronic superhighway*. New York: Thunder's Mouth Press.

Smetek, Ronald, Ronald Ostrom, and Joseph Croghan. 1991. Electronic deception - A variation on the Maskirovka theme. *American Intelligence Journal* 12, no. 1: 66-69.

Smith, Kevin B., Maj. 1994. The crisis and opportunity of information war. Monograph, School of Advanced Military Studies Fort Leavenworth, Kansas.

Stein, George J. 1995. Information warfare. *Airpower Journal* 4, no.1 (spring): 30-39.

_____. 1996. Information attack: Information warfare in 2025. Research paper, US Air War College, Maxwell Air Force Base, Alabama. Available from http://www.au.af.mil/au/2025. Internet accessed 26 July 26 1999.

_____. 1999. Battlefield of the future, Chapter 6. Website. Available, from http://www.airpower.Maxwell.af.mil/airchronicles/battle/chp6.html. Internet accessed 26 July 1999.

Sun Tzu. 1963. See Griffith. 1963.

Summe, Jack N., Lt Col. 1999. Information warfare, psychological operations, and a policy for the future. Thesis, US Army War College, Carlisle Barracks, Pennsylvania.

Szafranski, Richard, Col. 1995. A theory of information warfare: Preparing for 2020. *Airpower Journal* 9, no. 1 (spring): 56-65.

Thomas, Timothy L. 1996. Deterring information warfare: A new strategic challenge. *Parameters* XXVI, no. 4 (winter): 81-91.

_____. 1998. Dialectical versus empirical thinking: Ten key elements of the Russian understanding of information operations. *The journal of slavic military studies.* 11, no.1 (March): 40-62. Journal on-line. Available from http://call.army.mil/call/fmso/fmsopubs/issues/dialect.htm. Internet accessed 26 July 1999.

_____. 1999. Behind the great firewall of China: A look at RMA/IW theory from 1996 - 1998. Journal on-line. Available from http://call.army.mil/call/FMSO/fmsopubs/issues/chinarma.htm. Internet accessed 12 November 1999.

_____. 1999. Interview 12 November 1999 at the Foreign Military Studies Office, Fort Leavenworth, Kansas.

Timms, Ed. 1999. Unmanned aircraft earning wings over Balkans: Planes may offer glimpse at future of conflict. *Dallas Morning News*. Newspaper on-line. Available from http://ebird.dtic.mil/Oct1999/e19991025unmanned.htm. Internet accessed 25 October 1999.

Tirpok, John A. 1997. The New World of Information Warfare. *Air Command and Staff College, Correspondence Course*. CD ROM. Maxwell Air Force Base, Alabama: Air University, June.

Toffler, Alvin. 1970. *Future shock.* New York: Bantam Books.

_____. 1983. *Previews and premises*. New York: William Morrow and Company, Inc.

Toffler, Alvin and Heidi Toffler. 1993. *War and anti-war*. Boston: Little, Brown and Company.

_____. 1995. *Creating a new civilization: The politics of the third wave*. Atlanta, Georgia: Turner Publishing Inc.

Uchida, Ted T., Maj. 1997. Building a basis for information warfare rules of engagement. Monograph, School of Advanced Military Studies, Fort Leavenworth, Kansas.

U. S. Air Force. 1995. *Cornerstones of information warfare*. Washington, DC: U.S. Air Force.

_____. 1997. *Air Force doctrine document 1: Air Force basic doctrine*. Washington, DC: U.S. Air Force.

_____. 1998a. *Air Force doctrine document 2: Organization and employment of aerospace power*. Washington, DC: U.S. Air Force.

_____. 1998b. *Air Force doctrine document 2-5: Information operations*. Washington, DC: U.S. Air Force.

U. S. Air Forces in Europe. 1997. *Concept of operations for information operations*. Ramstein Air Base, Germany: U.S. Air Forces in Europe. Received from Mr. Suede Seegran, 32 AOS/AOW.

U. S. Army. 2000. *What is functional area 30?* Website. Available from http://www.cgsc.army.mil/dao/fa30/WhatisFA30.htm. Internet accessed 3 March 2000.

Verton, Daniel. 1999. Russia hacking stories refuted. *Federal Computer Week*. Newspaper on-line. Available from http://ebird.dtic.mil/Sep1999/ e19990928hacking.htm. Internet accessed 28 September 1999.

Vistica, George. 1998. We're in the middle of a cyberwar. *Newsweek*. Newspaper on-line. Available from http://ebird.dtic.mil/Sep1999/e19990913were.htm. Internet accessed 13 September 1999.

Wall, Robert. 1999. USAF expands information arsenal. *Aviation Week & Space Technology*. Newspaper on-line. Available from http://ebird.dtic.mil/Nov1999/ s19991117usaf.htm. Internet accessed 17 November 1999.

Warden John A. III. 1997. Air theory for the twenty-first century. *Air Command and Staff College, Correspondence Course*. CD ROM. Maxwell Air Force Base, Alabama: Air University, June.

Whitehead, YuLin, Maj. 1997. Information as a weapon: Reality versus promises. *Airpower Journal* 11, no. 3 (fall): 40-54.

39th Information Operations Squadron. 2000. *5th IO education and training requirements IPT action items*. Website. Available from http://www.hurlburt.af.mil/tenants/39ios/ipt.htm. Internet accessed 25 January 2000.

INITIAL DISTRIBUTION LIST

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

2. Defense Technical Information Center/OCA
   8725 John J. Kingman Rd., Suite 944
   Fort Belvoir, VA 22060-6218

3. Air University Library
   Maxwell Air Force Base, AL 36112

4. Major Randy Buddish
   Department of Joint and Multinational Operations
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

5. LCDR Gregory M. Landis
   Department of Joint and Multinational Operations
   USACGSC
   1 Reynolds Ave.
   Fort Leavenworth, KS 66027-1352

6. Dr. Graham Turbiville
   Foreign Military Studies Office
   604 Lowe Dr.
   Fort Leavenworth, KS 66027-2322

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 2 June 2000

2. Thesis Author: Maj James L. Griffith

3. Thesis Title: United States Air Force Information Operations Doctrine: Is It Relevant?

4. Thesis Committee Members Signatures: Randall W. Buddish, Maj, USAF
Gary M. Landin LCDR, USN
Glenn H. Tallia, Lt Col

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

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

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

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

EXAMPLE

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

Fill in limitation justification for your thesis below:

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

7. MMAS Thesis Author's Signature: [signature]

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

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

1. Foreign Government Information. Protection of foreign information.

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

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

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

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

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

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

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

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

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

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

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

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

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

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