Theses and Dissertations   Student Graduate Works

9-1998

A Descriptive Study of Information Operations and Information Warfare Awareness in the United States Air Force

Ryan D. Hollman

A DESCRIPTIVE STUDY OF INFORMATION
OPERATIONS AND INFORMATION WARFARE
AWARENESS IN THE UNITED STATES AIR FORCE

THESIS

Ryan D. Hollman, Captain, USAF

AFIT/GIR/LAS/98S-5

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/LAS/98S-5

A DESCRIPTIVE STUDY OF INFORMATION
OPERATIONS AND INFORMATION WARFARE
AWARENESS IN THE UNITED STATES AIR FORCE

THESIS

Ryan D. Hollman, Captain, USAF

AFIT/GIR/LAS/98S-5

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

AFIT/GIR/LAS/98S-5

A DESCRIPTIVE STUDY OF INFORMATION OPERATIONS AND

INFORMATION WARFARE AWARENESS IN THE UNITED STATES AIR FORCE

THESIS

Presented to the Faculty of the Graduate School of Logistics

and Acquisition Management of the Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Information Resource Management

Ryan D. Hollman, B.S.

Captain, USAF

September 1998

Approved for public release; distribution unlimited

Acknowledgments

This thesis was accomplished with the assistance of numerous individuals. The main guidance for this thesis was provided by my thesis advisor, Doctor Alan R. Heminger. Without Doctor Heminger's keen guidance and support, I could not have achieved this thesis. My sponsor, Major Robert Wicks, provided valuable input and direction for my research. My reader, Doctor Freda Strohrer, was instrumental in providing an outsider's view of my research. Her candid remarks ensured that this thesis was logically sound.

I also would like to thank the various individuals I contacted in conducting my research including Doctor Martin C. Libicki, Doctor Dan Kuehl, Colonel George Armstrong, and Doctor Fred Levien. These individuals took valuable time out of their schedules to offer their comments and suggestions for this thesis.

Last, but certainly not least, I would like to thank my wife, Dawn. Her unyielding love and support were necessary and greatly appreciated. I can never repay the sacrifices that Dawn has made and will continue to make as long as I am in the military.

Ryan D. Hollman

Table of Contents

v

List of Figures

List of Tables

AFIT/GIR/LAS/98S-5

Abstract

Information has always been important in military affairs, conflicts, and wars. Information warfare is an important new concept that is emphasized by the significance of computer and information technology. The United States Air Force has educated and trained individuals in information warfare since recognizing the importance of information warfare in 1995. The Air Force Information Warfare Center and the information warfare squadron were also created to address information warfare concerns. Information warfare is important to the entire Air Force. How familiar are Air Force people generally in information warfare? This thesis addresses awareness of information warfare and information operations concepts.

Despite the amount of focus, training, and education, it was unknown how aware individuals were concerning information warfare and information operations. This thesis surveyed eight hundred officers and enlisted personnel with a response rate of 214 to determine the baseline of information warfare awareness.

Approximately sixty percent of the respondents indicated that they were aware of information warfare. Also, individuals who received information warfare training responded higher than individuals without training. This is the first study in information warfare and information operations awareness. Additional research is needed to determine how the awareness levels are changing and the effectiveness of the training.

A DESCRIPTIVE STUDY OF INFORMATION OPERATIONS AND

INFORMATION WARFARE AWARENESS IN THE UNITED STATES AIR FORCE

I. Introduction

There's a war out there...a world war. And it's not about who's got the most bullets, it's about who controls the information: what we see and hear, how we work, what we think. It's all about the information.
 - Ben Kingsley as "Cosmo" in <u>Sneakers</u> (27)

Information

Information has always been a vital resource in battles, conflicts, and wars. "Competition for information is as old as human conflict" (8: 1). Technology directly affects the importance of information. In the fourteenth and fifteenth centuries, lanterns and signal mirrors were used to transmit information over line-of-sight distances and communicate instructions about battle plans and warn of enemy attacks. The printing press was invented in the seventeenth century and dramatically changed how information could be stored, copied, and shared. The technological advances of the twentieth century include telephones, radio, radar, encryption, satellites, microprocessors, and computers. These inventions have brought us into the "information age." Now the importance of information grows as rapidly as the information technology itself. With this growth in importance, vulnerability to an attack on information also grows. Accordingly, how we deal with information is more important every day.

The policies and procedures of warfighting have been greatly influenced by the information technological revolution of this century. The advances in computer microprocessors, mass storage devices, and telecommunications have changed the nature

1

of information warfare. The military's policies and military personnel may not be keeping up with the rapid pace of technology advancement. The United States Air Force (AF) is working to incorporate information as a vital resource and information warfare into its basic doctrine and to enlighten all Air Force members on the importance of information as a resource and information warfare.

What is information? According to the Oxford American Dictionary, information is "facts told or heard or discovered" (10: 338). The Air Force defines information in its Cornerstones of Information Warfare document as observable facts or events, which must be perceived and interpreted (8: 2). Cornerstones of Information Warfare also states that information is perceived phenomena or data and the instructions on how to interpret the data, thus giving the data meaning (8: 2). Information is just as important as it was centuries ago; however, computer technology has changed how we, as individuals, perceive and interpret information.

This thesis investigates and measures the individual Air Force member's understanding of information-warfare items, specifically including information superiority, information operations, and information warfare. Information provides the basis for decisions we make. Air Force Doctrine Document 2-5 (AFDD 2-5), Information Operations, states that "the possession and manipulation of information itself is a key element of the war-winning equation" (9: 1). Sun Tzu, a warrior from ancient China, also stated "Know the enemy and know yourself; in a hundred battles you will never be in peril" (30: 84). In conflicts and wars, the side with the better information about the battle will most likely be victorious.

Information Superiority

The Chairman of the Joint Chiefs of Staff (JCS) identified information superiority as an emerging area of importance for the joint arena. The Joint Chiefs of Staff defines information superiority as "the ability to collect, control, exploit and defend information while denying the adversary the same" (31: 16). Air Force leadership also perceives the importance of information superiority, and therefore identifies information superiority as one of six Air Force core competencies. The Air Force defines information superiority as "that degree of dominance in the information domain which permits the conduct of friendly operations without effective opposition" (9: 40). While the Joint Chiefs of Staff and Air Force definitions vary in detail, they are similar in that both conclude that information is a critical resource.

For information superiority to be realized, however, individuals must be aware of it, understand it, and know how to use it. Some military members do not understand or know about the concept of information superiority. If they are aware of the concept of information superiority, they may not know how to accomplish it in Air Force operations. This predicament itself may hinder the goal of having information superiority in conflict, much less in peacetime.

Information superiority is vital not only to the other core competencies of the Air Force, but also to the full spectrum dominance described in JV 2010 (31: 19, 7: 3). Full spectrum dominance is composed of four concepts: dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. These four concepts are intended to enable the military to dominate the full range of military operations including humanitarian assistance, peace operations, and full-scale conflict (31: 25). Full spectrum

3

dominance is defined by the Joint Chiefs of Staff as "The ability to dominate any adversary and control any situation in any operation across the range of military operations" (15: 84).

The other Air Force core competencies include air and space superiority, global attack, rapid global mobility, precision engagement, and agile combat support. Of the six AF core competencies, information superiority "is the Air Force core competency upon which all other core competencies rely" (7: 3).

The United States depends more on information and information technology than any other military in the world right now (1: 100, 26: 3). This dependency makes the US more vulnerable to an attack on its information and information systems than any other country (23: 29, 20: 9-17). Therefore, the military must not only identify information superiority as a core competency; it is important that military members understand what information superiority is and how to achieve and sustain it.

Information Operations

Information superiority is achieved via information operations (IO). Information operations are "those actions taken to effect [sic] adversary information and information systems while defending one's own information and information systems" (7: 1). Three components are required for information superiority: information systems, information operations, and relevant information (15: 39). Information systems are the tools for collecting, analyzing, and dissemination information (15: 39). Relevant information is having the right information in a timely manner (15: 40). Information operations and its subset, information warfare, are fundamental to achieving and sustaining information superiority.

Information operations are composed of three main activities. The first is gaining information through surveillance, reconnaissance, and intelligence gathering methods. The second activity is exploiting information or using information to the best of one's ability, whether from intelligence analysis, weather, navigation and positioning, command and control, communication, or computers. The third activity consists of attacking and defending information operations (7: 1).

The offensive and defensive portions of information operations are defined further in the draft of AFDD 2-5. Offensive information operations include psychological operations (PSYOP), electronic warfare (EW), military deception, information attack, and physical attack. Defensive information operations include security measures, counter-deception, counter-intelligence, and counter PSYOP (9: 8).

Just as information has existed in warfare since the beginning of human conflict, so have many of the offensive and defensive areas listed above. While all of these areas are affected by technology, two are largely created by recent developments in information technology: information attack and portions of security measures. Information attack comprises "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" (9: 13)

Information operations occur constantly. A military must constantly be preparing for conflict lest it be caught unready. Information and computers must be protected from various threats such as computer viruses, natural disasters, power failures, software errors, and other such intentional or unintentional hazards. Information operations do not stop when a country is involved in conflict; however, the subset of information operations

5

that does occur during conflict is called information warfare. According to AFDD 2-5, "information warfare, which has both offensive and defensive components, is information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (9: 3).

Information Warfare

Information warfare (IW) is referred to by numerous terms including "infowar," "netwar," "command and control war (C^2W)," "third-wave war," "knowledge war," and "cyberwar" (1: 100). Although these terms vary in meaning, the emphasis, nevertheless, is the same: information, in one form or another, is a weapon or a target of information warfare.

In the AF definition, information warfare is related to information operations as air warfare is related to air operations. Operations are conducted across the spectrum of conflict including peace, crisis, war, restoration, and peace again. Warfare only occurs during times of crisis and war. Information operations actions taken to acquire, transmit, store, or transform information conducted during crisis or war to achieve information superiority and specific military objectives become information warfare (7: 1).

The difference that recent technology has had on information and warfare is that in the past information was used as a tool of warfare. Now information itself is a separate realm, a potent weapon, and a lucrative target (1: 101, 23: 27). Information technologies have changed warfare as much as the armored tank changed warfare in World War I. Future war, information war, "is believed by many to be the means by which the next 'big' war will be fought and, more importantly, the means by which future wars will be won" (1: 99).

Air Force Focus on Information Warfare Training

In August 1984, the Chief of Staff of the AF directed the Air Education and Training Command (AETC) to develop formal courses educating officers and enlisted troops about information warfare. The AF currently teaches information warfare concepts at Air University's College of Aerospace Doctrine, Research and Education (CADRE) Information Warfare Application Course (IWAC). This course targets AF members from E-6 (Technical Sergeant) to E-9 (Chief Master Sergeant), O-3 (Captain) to O-5 (Lieutenant Colonel), and equivalent civilian grades and gives them a one-week overview of what information warfare is and how to implement information warfare in the AF. CADRE also directs a Senior Information Warfare Application Course (SIWAC) aimed at educating senior AF leaders O-6 and above (Colonels and Generals). However, IWAC courses are limited to ten courses per year with 72 people per course. Therefore, IWAC will not be able to educate all AF members firsthand in a timely manner. CADRE will continue to teach IWAC until senior leaders decide that AF members and organizations understand and implement information warfare concepts at an undetermined level as of yet.

My research for this thesis found that no one has an overall general measurement of information warfare understanding in the AF. Members may also be unaware of Information Superiority as an AF core competency or how information operations and information warfare relate to Information Superiority.

The Problem

The AF has decided that the importance of information operations and information warfare warrants development of specific doctrine (AFDD 2-5), training via

CADRE, and even organizations such as the Air Force Information Warfare Center (AFIWC) and the 609th Information Warfare Squadron. However, in spite of the training discussed above, the current knowledge level of AF members' toward information operations/information warfare is not readily known (32). Individual units, such as CADRE, may know how many members that it has taught; they do not, however, know how many members still need training or education. Information operations and information warfare are taught at various levels and various schools from basic training and unit training to Air Command and Staff College (ACSC). Leaders may not fully know if AF members understand the current AF definitions, policies, and doctrine pertaining to information operations and information warfare. AF members may not know the difference between information operations and information warfare. Even if members do know what information operations and information warfare are and the differences between the two, they may not know or understand how the offensive and defensive aspects of information operations/information warfare affect them. Members may also be unaware of Information Superiority as an AF core competency or how information operations and information warfare relate to Information Superiority. Finally, due to the numerous methods of training available leaders may not know how many members have been trained in information operations and information warfare concepts either through IWAC or through SIWAC, or from other means such as self-taught or other service schools.

The goal of this research is to present a current snapshot of AF personnel awareness of information warfare concepts and issues. This snapshot is useful in determining where we are now and for future training evaluation and research. Six

8

research questions developed for this thesis are listed following this paragraph. It is intended that this research will present a baseline of IO and IW understanding so that senior leadership can make better-informed decisions. It may also prove useful to enhancing IWAC curriculum; if CADRE leaders know what AF members perceive information operations and information warfare as, then they can better focus their course.

Research Question 1: To what extent are AF members aware of the current AF definitions of information operations and information warfare?

Research Question 2: To what extent are AF members aware of how information operations and information warfare affect them?

Research Question 3: To what extent are AF personnel aware of the differences between offensive and defensive information operations/information warfare?

Research Question 4: To what extent are AF members aware of how Information Superiority links to information operations/information warfare?

Research Question 5: To what extent have AF members been formally trained on information operations and information warfare and by what system?

Research Question 6: To what extent does information operations/information warfare training improve the awareness of information warfare in AF members?

Overview of the Research

Chapter II explores the current body of literature pertaining to this research. Chapter III describes the nature and technique and the research assumptions made to compile a survey necessary to answer each research question. Chapter IV presents the results of the survey data for each research question. Finally, Chapter V discusses the

overall results of this research in attempting to baseline the current attitudes and perceptions of AF members toward information warfare. It also identifies limitations of the study and makes suggestions for further research.

II. Literature Review

This chapter documents the exploration of current information warfare research to attempt to find previous similar studies. In this chapter, I identify the resources used to search libraries, databases, and the Internet to find information warfare research. Information operations and information warfare organizations and individuals were also contacted either via telephone or via e-mail collect information for this thesis and to ask if they knew of any related research.

What I Found

I found no specific research measuring the IW or IO awareness levels of individuals within the Air Force. However, there is a great deal of research on information warfare, information operations, and information superiority in general. In the following paragraphs, I summarize current literature about the differences between information warfare and information operations including the differences between them. I also explore the differences between past and current information warfare. The third area discussed is the need for individuals to be aware of IO, IW, and information superiority. Finally, I outline how core competencies relate to IO and IW.

Information Warfare versus Information Operations

Information warfare and information operations may seem very similar or the same to someone unfamiliar with IW and IO. The definitions of IW and IO are even similar. AFDD 1, AF Basic Doctrine, defines IO as "those actions taken to affect adversary information and information systems while defending one's own information and information systems" (6: 81). Meanwhile, IW is defined as "actions taken to achieve

information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks" (6: 81).

(14: IW 110 Slide 31)
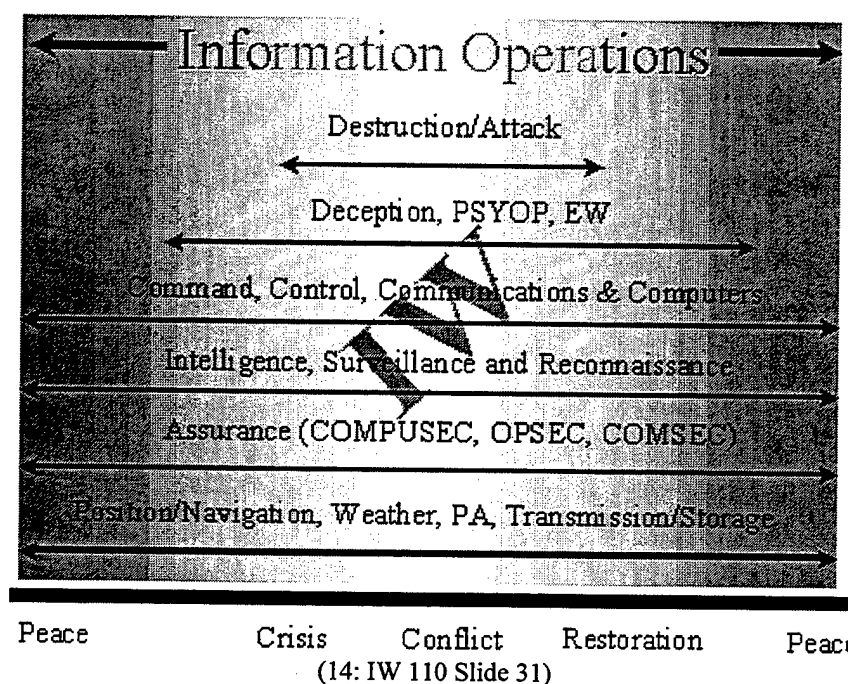
Figure 1: Information Operations and Information Warfare Overlap

The Air Force further clarifies the definition of IW in AFDD 1 as "information operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries" (6: 81). This is also the definition for IW used in AFDD 2-5 (9: 40). Figure 1 shows how IO and IW overlap. Information operations occurs during the entire spectrum from peace, crisis, conflict, restoration, back to peace. Information warfare occurs during crisis, conflict, and resolution only. Some activities such as destruction/attack and deception, psychological operations (PSYOP), and electronic warfare (EW) transpire more during IW and the remaining activities

12

happen during both IO and IW (14: IW 110 Slide 31). However, the division between IO and IW is imprecise.

Another possible differentiation between IW and IO is achieved by separating the offensive and defensive portions of IW and IO. AFDD 2-5 categorizes offensive information operations to include PSYOP, EW, military deception, physical attack, and information attack. Defensive IO includes security measures, counter-deception, counterintelligence, and counter-psychological operations (9: 7-17). I could not find any documentation stating that offensive IO/IW took place only at certain times, such as during crisis or conflict. Likewise, I could not find any documentation stating that defensive IO/IW was conducted continuously.

Past versus Current Information Warfare

Information warfare of the past is greatly different from current information warfare. Martin Libicki, notable author of <u>What Is Information Warfare</u> (22) and <u>Defending Cyberspace and Other Metaphors</u> (20), wrote about the various forms of IW and which of them are new. Command and control systems have benefited from new technologies and have shifted the focus from commanders to the command systems. Electronic warfare has been around since World War II but benefit from technological advances. Psychological operations have remained the same since ancient times but television and the Internet are new media to transmit PSYOP. Libicki states hacker warfare, economic warfare, and cyber-warfare are the newest areas of IW and are results of modern technology including computers and telecommunications (22: Chapter 10, 22: 65-73).

What else is new about information warfare? Libicki also states that the U.S. is becoming more dependent on information systems. Information systems are increasingly interconnected by telecommunications (22: 11). "The more a nation depends on the integrity of its information infrastructure, the more it can be put at risk by attacks there" (22: 12). The leading edge of technology makes the United States more vulnerable to an information attack than less developed countries. Pat McKenna writes, "Although Somalia isn't susceptible to an info attack, the United States is" (23: 29). According to McKenna, both Major General Michael Hayden, commander of Air Intelligence Agency (AIA), and Colonel Frank Morgan, commander of the Air Force Information Warfare Center (AFIWC), agree that the U.S. is the most vulnerable country in the world (23: 29).

Arsenio Gumahad, Lieutenant Colonel USAF, states, "The use of information in war has been a basic warfighting requirement throughout history. Technology has made information more available, and now it may become the weapon of choice" (12: 14). He goes on to state advanced societies depend on infrastructure including telephone networks, electric power grids, and the Internet. Adversaries only need be knowledge of these systems and target them to cause massive damage (12: 15).

The differences of information warfare from the past to information warfare now and in the future are evident. The previous paragraphs outline how the technological growth of computers and telecommunications makes information warfare unlike before. The main difference is modern information warfare is dependent on modern information technology.

Individuals Need to be Aware

Gumahad declared, "The high-tech military of the future will be smaller but more sophisticated and specialized" (12: 17). He goes on to state military members will be well trained, skilled warrior-technicians who operate advanced electronic gadgetry. Information will enhance operations on the battlefield. Gumahad maintains doctrinal and organizational changes must occur for the technical evolution to transpire (12: 17).

Dr. Dan Kuehl of the National Defense University discusses IW awareness issues in his article, "Educating the DOD About Information Warfare: Is the Glass Half Full, or Half Empty?" In this article, Dr. Kuehl states, "The four operational concepts set forth by JV 2010—dominant maneuver, precision engagement, focused logistics, and full-dimensional protection—rest on a base on information superiority" (16). He also points out that two of the five chapters from "Expanding JV 2010" focus on information superiority and joint operations in the information age (16). Finally, Dr. Kuehl remarks that "We need to study IW because this is the way we will fight in the future" (16).

Former Air Force chief of staff, General Ronald Fogleman, commented about the importance of information in a speech. He said, "One thing that is no secret is the importance of information…The technology information explosion in our society has created an awareness of the power of information" (11). General Fogleman states later, "I think this information explosion is going to allow dramatic changes in how this nation fights…soldiers, Marines, sailors and airmen on the front lines will see and exploit opportunities as they occur" (11). General Fogleman's remarks point out that not just the leaders and Generals need to be aware or knowledgeable of IO and IW, but military members at all levels must know and understand the value of information and

information warfare. The AF's recognition of the value of information is also reflected in its inclusion of information superiority as an Air Force core competency.

Core Competencies

Air Force Basic Doctrine (AFDD 1) defines a core competency as follows:

> The basic areas of expertise or the specialties that the Air Force brings to any activity across the spectrum of military operations whether as a single Service or in conjunction with the core competencies of other Services in joint operations. Core competencies represent both air and space power application theory and physical capability represented in a well-trained and equipped air force. (6: 80)

The Air Force's core competencies include six items: rapid global mobility, precision engagement, global attack, air and space superiority, information superiority, and agile combat support (6: 28). As stated in Chapter I, information superiority is vital to the other five core competencies. In addition, information superiority is necessary for the full spectrum dominance described in JV 2010 (31: 19, 7: 3).

Sources of Information

Several libraries and online research databases were searched to review the published books, technical reports, theses, and journal articles to try to find any research on measuring the awareness, knowledge, or understanding of information warfare by individuals.

EBSCO. EBSCO is an online database, available by subscription only, of over five hundred journals, abstracts and indexing for over three thousand-one hundred scholarly journals, and coverage of the Wall Street Journal, The New York Times, and The Christian Science Monitor. Searches of this database did not reveal any previous research similar to this thesis.

16

FirstSearch. FirstSearch is another online research database, available by subscription only. FirstSearch has approximately 12,500 journals in science, technology, medicine, social science, business, humanities, and popular culture. Searches of the science and technology databases were unable to discover similar research.

Library of Congress. The Library of Congress catalog is available via the Internet at http://lcweb.loc.gov. Searches of the catalog revealed no new sources for this thesis.

Other. Various city, military, and university libraries, which were available in either the physical area or the Internet, were searched. A great deal of reference material for this research was found through all the available sites, including EBSCO, FirstSearch, and the Library of Congress. I found no previous research measuring the information operations or information warfare awareness levels of individuals.

Organizations and People Contacted

Many different organizations and people familiar with Information Warfare and Information Operations research were contacted to learn whether any previous research had been conducted on awareness of information warfare. The organizations and individuals contacted are listed in the following paragraphs.

CADRE/IWAC: Major Robert Wicks, IWAC Chief, was contacted and was unaware of any similar research being conducted. Major Wicks suggested contacting the National Defense University, the AF Information Warfare Center, and the Fleet Information Warfare Center of the Navy (32).

National Defense University (NDU): Martin C. Libicki, noted author of What is Information Warfare? (22) and Defending Cyberspace, and Other Metaphors (20), was unaware of any research of information operations/information warfare that measured

17

awareness of individuals (21). However, he suggested contacting two of his colleagues: Dr Fred Giessler and Dr. Dan Kuehl. Dr. Dan Kuehl was also unaware of any specific studies but made several more recommendations for contacts including Fred Levien at the Naval Postgraduate School, Colonel George Armstrong at Armed Forces Staff College, and the US Air Force Academy's information warfare course (17, 18).

Air Force Information Warfare Center (AFIWC): Capt Pearce of AFIWC was also questioned about information warfare awareness research. He also was unaware of any such research to date. He suggested contacting the AF Computer Emergency Reaction Team (AFCERT) to see if they had conducted any such research (24). AFCERT negatively replied about having any such information: "AFCERT does not conduct Information Warfare (IW) awareness research" (13). Captain Pearce also suggested contacting Capt Dan Drumend of NAIC/AI (24).

Armed Forces Staff College's IW Course: AF Colonel George Armstrong was contacted at the Armed Forces Staff College (2). Colonel Armstrong recommended a previous AFIT thesis by Captain Kenneth Peifer, An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy. A further review determined that Captain Peifer's thesis focused on determining if unclassified current and pending AF IW and IO doctrine and policy is moving in a positive direction (25). It dealt with official policy and doctrine and did not measure or survey individual AF member's awareness of information warfare. Policy and doctrine are the direct result of AF leaders' views on IW and IO and therefore it serves as a basis for what AF leaders currently regard IW and IO as. Colonel Armstrong also

recommended Joint Publications 3-13 and 3-13.1. Colonel Armstrong was unaware of any similar IW awareness research (2).

Naval Postgraduate School: I also contacted Dr. Fred Levien of the Naval Postgraduate School. Dr. Levien is the Chairperson of the Information Warfare Academic Group. Dr. Levien was also unaware of any research similar to mine (19). He did suggest that I review Roger Thrasher's thesis, Information Warfare: Implications for Forging the Tools (29). Roger Thrasher used a group of experts to discover and examine information warfare acquisition issues.

United States Air Force Academy: Lieutenant Colonel John Becker was contacted at the United States Air Force Academy. Lieutenant Colonel Becker teaches a course on "Ethics and Information Warfare." Lieutenant Colonel Becker was unaware of any previous research that measured or surveyed individuals' awareness of IW (3).

The lack of any similar research on measuring individuals awareness, understanding, or knowledge of information warfare permits this current research freedom in choosing research methodology and survey instruments. However, since this research is exploratory, there will be no immediate external validation method available. Chapter III discusses the methodology of this thesis in detail.

III. Methodology

Focus of the Study

This research is primarily descriptive inasmuch as individuals' awareness of information warfare had not been previously studied. In addition, there was a general lack of quantitative research in the information warfare field. Cooper and Emory define the objective of a descriptive study as "to learn the who, what, when, where, and how of a topic" (4: 121-122). This research was also somewhat exploratory since researchers have not investigated what individuals know about information warfare. The research questions in Chapter I cover the who, what, and how of information warfare awareness. Determining the answers to the seven research questions appeared to fit well within the parameters of an exploratory study.

The data for this research was gathered by surveying a sample of AF enlisted members and officers. The survey was mailed out to a randomly selected group of members. As of 30 June 1998, the AF had 68,636 officers (O-1 through O-6) and 293,354 enlisted for 361,990 total members, not including Colonels and General officers. According to the equation below, the sample size needed for 95-percentile confidence interval was 384 members. Past response rates for AF members were about 50 percent; therefore, the sample size needs to be doubled to at least 768 members (28).

Sample Size Determination: $\quad n = \dfrac{N(z^2) * p(1-p)}{(N-1)(d^2) + (z^2) * p(1-p)}$

n = sample size required
N = population sample size (= 361,990 for AF population)
z = factor of assurance (= 1.96 for 95% confidence interval)
p = maximum sample size factor (= .50)
d = tolerance (= .05)

Developing the Survey Instrument

To develop a survey instrument, several questions were created to address each of the research questions. Demographic questions such as rank of the respondent and his or her major command (MAJCOM) were also included. The survey is available in appendix B. Pretesting was accomplished to refine the survey questions. The thesis advisor, sponsor, and subject experts were consulted for initial revision. After approval at this level, the survey was presented to a small group of research peers for final revision.

Pretesting and Validating the Survey Instrument

The survey was presented to a pretest group in order to further refine question meaning, wording, continuity and flow, question sequence, and to determine to length of time required to complete the survey. The process was repeated as needed to refine each question.

Once this was completed, the survey was submitted to the AF Personnel Center. According to AF Instruction 36-2601, all AF surveys need the approval of Headquarters AF Personnel Center (5: 1). This survey was approved by HQ AFPC before being sent out. The approved survey is available is appendix B.

Once approved, the survey was sent out to the randomly selected AF members. A waiting period of four weeks was given for the survey to be delivered, completed, and returned.

Data from the surveys was entered into a computer statistically program for processing. Descriptive statistics including the means, standard deviations, 95 percent confidence intervals, minimums, and maximums were calculated from the response data and further discussed in Chapter IV.

IV. Results of Analysis

Chapter IV discusses the results and comments compiled from the surveys returned. Results are grouped by categories such as information warfare awareness, offensive versus defensive IO, training, etc. First, the general results, such as response rate and demographics, are discussed.

General Results

Out of the 800 surveys sent out, 214 surveys were returned with useful responses for an overall response rate of 26.75 percent. The surveys were grouped into either officer or enlisted. Officers were sent 200 of the surveys while enlisted were sent 600 surveys. The response rate for officers (O-1 to O-5) was 36 percent (72 surveys returned). Enlisted response rate was 23.7 percent (141 surveys returned). One individual did not indicate his or her rank. The ratio of officers to enlisted was 33.6 percent officers and 66.4 percent enlisted. The responses rates for officers and enlisted, individually as well as overall, were considered acceptable.

Individuals were also requested to report their total active federal military service (TAFMS) in years completed. TAFMS is how many years that individual has served the military on active duty. The average TAFMS was 10.98 years. The range was from zero years to 27 years. Tables 1 and 2, following this paragraph, summarize information on frequency and percent of responses by rank and major command, respectively.

Table 1: Frequency Distribution by Rank

Rank	Frequency	Percent of Respondents
Field Grade Officer	40	18.8
Company Grade Officer	32	15.0
Senior NCO	25	11.7
NCO	58	27.2
Airman	58	27.2
TOTAL	213	100.0

Table 2: Frequency Distribution by Major Command

Major Command	Frequency	Percent of Respondents
ACC	56	26.3
AETC	26	12.2
AFMC	21	9.9
AFSOC	13	6.1
AFSPC	14	6.6
AMC	30	14.1
PACAF	18	8.5
USAFE	12	5.6
Other	23	10.8
TOTAL	213	100.0

Information Warfare Awareness

Questions 4 through 7 in the survey were designed to measure how aware

individuals thought they were about information warfare. Overall, 63.5 percent of

respondents (134) agreed or strongly agreed that they were aware of the concept of IW,

understood the definition of IW, and thought the AF's definition of IW was useful.

Individually, 81.7 percent of respondents (174) either agreed or strongly agreed that they

were aware of the concept of IW. Eighty-five point nine percent of respondents (183)

agreed or strongly agreed that they understood the AF's definition of IW. Sixty-eight

point six percent of respondents (146) agreed or strongly agreed that the AF's definition

of IW was useful. Finally, 3.3 percent of respondents (7) had a different definition of IW.

A one-way ANOVA (Analysis of Variance) was performed with the dependent variable of IW awareness (questions 4-7) and categories of officer/enlisted and training. Officers and enlisted were statistically significantly different groups for IW awareness. Officers had a higher mean (12.129) than enlisted (11.177) at an alpha of 0.01 ($p = 0.0003$). Training was also a statistically significant category for IW awareness. Individuals who received training had a higher mean (12.311) than those who did not receive training (mean = 11.074) at an alpha of 0.01 ($p = 0.0000$). Finally, years of service (TAFMS) was checked with least squares linear regression to see if TAFMS correlated with IW awareness. TAFMS failed to add any statistically value to IW awareness.

The individuals with a different definition reported their own IW definition or comments. A collection of the definitions is offered below.

> "Our ability to exploit information systems to our benefit and denying our enemies the same."

> "Information warfare involves improving the usefulness of our information while decreasing the usefulness of an adversary's information."

Individuals' comments are summarized here.

> "Sounds the same as IO definition, but with more extraneous words. I would think IW is a strategic approach or methodology, not just actions, which are really operations."

> "... Your IW definition is missing some key items. As they are stated, it is not apparent that IW is a subset of IO."

> "Common sense. Military definitions try to make perfect sense, however are nothing but the same definition written differently rambling one after another. Info warfare is common sense. I don't have the perfect definition, but the Air Force's definition is not."

> "Just need to add security in the statement."

> "Too vague or is this for reasons of security."

<u>Information Operations Awareness</u>

The next category of questions on the survey explored IO awareness. Questions 8 – 11 directly measured IO awareness and questions 16, 17, and 30 also contributed to measuring IO awareness. A paired T-test was used to measure the difference between IW awareness and basic IO awareness (questions 8 – 11). The T-test did not show any statistically significant differences between IW awareness and IO awareness. Sixty point six percent of respondents (126) agreed or strongly agreed with the questions measuring basic IO awareness. The expanded IO awareness measure (including basic IO awareness plus questions 16, 17, and 30) indicated that only 43.3 percent of the respondents (88) agreed or strongly agreed with all IO awareness questions. Seventy-six point nine percent of respondents (163) agreed or strongly agreed that they were aware of the concept of IO. Eighty-one point seven percent of individuals (175) understood the AF's definition of IO. Sixty-six point three percent of individuals (142) thought the definition was useful. Sixty-five point five percent of respondents (137) thought IO affected them at work while 73.5 percent (153) thought IO affected their organization. Finally, 79.2 percent of respondents (167) felt IO supported information superiority.

ANOVA tests for basic and expanded IO awareness were conducted for officer/enlisted, major command, and training categories. Again, officers (mean = 11.829) had statistically higher responses than enlisted (mean = 11.065) regarding basic IO awareness, with alpha = 0.01 (p = 0.0064). However, expanded IO awareness failed to reveal a statistically significant difference. Individuals that received training had statistically higher responses for both basic and expanded IO awareness. Major command did not statistically correlate with responses for either basic or expanded IO

awareness. Linear regression models did not reveal any statistical significance to
TAFMS and either basic or expanded IO awareness.

Only a handful, 1.4 percent, of the respondents (2) had a different IO definition or
comments. These comments are listed below:

> "Needs to be better differentiation between IW and IO."

> "Same thing [as IW definition]. It's basically a sentence taken from info
> warfare with a few words changed. Unoriginal and poorly thought out. The definition is
> simply to use common sense while working."

Research Question 1: Extent of IO/IW Awareness

To what extent are AF members aware of the current AF definitions of
information operations and information warfare? The previous sections on IW and IO
awareness apply to this research question. To summarize the results, 63.5 percent of
individuals (134) indicated that they were aware of IW concepts and definitions. Sixty
point six percent of the respondents (126) indicated that they were aware of the basic IO
concepts and definitions. Finally, 43.3 percept of AF individuals (88) agreed or strongly
agreed with questions measuring expanded IO concepts.

Air Force Basic Doctrine Document 1

AFDD 1 was the source of all definitions used in the survey to measure IO/IW
awareness. Therefore, a question asking individuals if they were familiar with the
information in AFDD 1 was asked. Only 34.3 percent of respondents (73) were familiar
with AFDD 1. Almost half, 48.3 percent, of the respondents (103) were not familiar with
AFDD 1. The remainder, 17.4 percent (37), responded neutrally to the question. The
only category that statistically separates respondents on their knowledge of AFDD 1 was
whether they had received training. Individuals that received IO/IW training were more

familiar with AFDD 1 than individuals who did not receive training (mean 3.24 versus 2.59, alpha = .01, p = 0.00).

Information Warfare/Operations Differences

Individuals were asked if they thought that IW and IO were different. Most people, 56.4 percent (120), agreed or strongly agreed that IW was different from IO. Twenty-one point two percent (45) disagreed that IW and IO were different. The remainder, 22.5 percent (48), neither agreed nor disagreed. ANOVA tests did not reveal any statistically significant categories from officer/enlisted, major command, or training.

Research Question 2: Information Operations/Warfare Effects

Questions 16 and 17 asked individuals if they thought IO affected their individual job and their organization, in that order. Most individuals, 63.4 percent (132), thought that IO affected both their job and their organization. Neither officer/enlisted nor TAFMS categories statistically contributed to IO effects. However, major command did contribute to individual perception of IO effects. Individuals from AFSOC (mean = 8.08) and ACC (mean = 7.72) reported effects statistically higher than individuals from AETC (mean = 6.15), alpha = .01, p = 0.0009. The training category also statistically contributed to IO effects. Individuals who received training reported statistically higher scores (mean = 7.92) than individuals who did not receive training (mean = 7.02), alpha = .01 and p = 0.0003.

Sixty-five point five percent of individuals (137) agreed or strongly agreed that IO affected their job. Meanwhile, 73.5 percent of individuals (153) agreed or strongly agreed that IO affected their organization. A paired T-test performed between questions

16 and 17 to see if there was any statistically significant difference between IO affects for individuals and for organizations, showed statistically higher scores for IO effects on organizations than on their individual jobs (question 17 mean – question 16 mean = 0.1538, p =0.0001).

Research Question 3: Offensive/Defensive Information Operations Differences

Questions 18 – 28 focused on measuring the differences between offensive and defensive IO. Most individuals, 69.8 percent (145), agreed or strongly agreed that they were aware of the differences between offensive and defensive IO. Individuals who received training reported statistically higher scores than those who did not receive training (training mean = 3.97 versus no training mean = 3.44, p = 0.0000). The categories of rank, officer/enlisted, and major command did not statistically influence question 18.

Questions 19 – 28 asked individuals to report if they thought offensive or defensive IO included each of the following: psychological operations, electronic warfare, military deception, physical destruction, or information attack. Paired t-tests were performed for each offensive and defensive area. Individuals reported statistically significant higher scores for offensive IO including PSYOP than defensive IO. Individuals also reported higher scores for offensive IO including military deception and physical destruction than for defensive IO.

Overall, 45.9 percent of individuals (94) reported no difference between what offensive IO and defensive IO contained. Sixteen point six percent of individuals (34) reported that defensive IO included more operations than offensive IO. Thirty-seven

point five percent of individuals (77) thought offensive IO included more operations than defensive IO.

Research Question 4: Information Superiority

Survey questions 14, 15, 29, 30, and 31 measured aspects of information superiority (IS) awareness. Overall, most respondents, 55.1 percent (113), agreed or strongly agreed with IS awareness questions. About four-fifths of people agreed or strongly agreed that both IW (80.7 percent, 172) and IO (79.3 percent, 169) contribute to IS. Seventy point two percent of individuals (146) agreed or strongly agreed that they were aware of IS as defined by the AF. Responses for questions 15 and 30, which stated that IO contributes or supports IS, were not statistically significant (79.3 percent versus 79.2 percent agree or strongly agree). Finally, 70.1 percent of respondents (148) agreed or strongly agreed that information superiority is necessary for air superiority. One respondent commented that "no [IO is not necessary], but without information superiority, air superiority becomes exponentially more difficult to maintain."

Training was the only statistically significant category for determining IS awareness. Individuals who had IO/IW training responded higher (mean = 19.93) than individuals without training (mean = 18.62), p = 0.0011. Categories of officer/enlisted, rank, major command, and TAFMS were not statistically significant for determining levels of IS awareness.

Research Question 5: Information Operations/Warfare Training

Many individuals responded that they had received IW/IO training (35.4 percent). Of these individuals, 68.5 percent of individuals (50) said they received their training

29

from their unit or organizational in-house training. The remaining 23 individuals (31.5 percent) received their training from an assortment of sources, which are discussed in the next paragraph. Sixty point seven percent of people (94) said they agreed or strongly agreed that it would be valuable for them to receive initial training or additional training.

There are many avenues available for military members to receive training in either IW or IO. The following educational courses and schools were listed in addition to the responses listed on the survey: Air Command and Staff College (ACSC), Squadron Officers' School (SOS), Information Warfare Planning Group at Osan AB Korea, AFSOC School, NCO Academy, Air War College (AWC) course, Airmen Leadership School (ALS), and SHAPE Belgium (NATO). Many of these listed are formal Professional Military Education (PME) courses available for either officers or enlisted.

Research Question 6: Impact of Information Operations/Warfare Training

What is the impact of IO/IW training? A summary of what criteria are affected by training include: IW awareness, IO awareness (both basic and extended), AFDD 1 awareness, how IO effects individual job and organization, difference between offensive and defensive IO, PSYOP, EW, military deception, and information superiority. Individuals with training responded statistically higher on all of these criteria than individuals without training. The individual tests and results for the impact of training are in the preceding sections.

Comments

Thirty-nine respondents (18.2 percent) offered comments either at the end of the
survey or during the survey. Eight respondents appeared to be in favor of IW/IO training.
Comments in favor of training are listed below:

> "Information operations/warfare should be incorporated into the career
> development courses as well. [It] should be taught at lowest level possible – basic, OTS,
> tech schools."

> "Yes. It would be beneficial to receive IW training. However, it should be short
> enough (1-2 hours only) not to interfere with all of the other requirements aircrew
> members have to meet."

> "I feel everyone could benefit from IW training. COMPUSEC/SATE already
> contribute, with the terroristic acts by hackers, we – in the USAF, are under 'attack'
> daily."

> "To understand IW there should be a mandatory training session when you get
> to your duty station."

> "Concepts need to be core parts of ACOT and BCOT."

> "Security is a joke at [my base]. Information integrity is compromised everyday
> here. A serious look needs to be given at [my base's] security. More training needs to be
> given to System Administrators."

> "It would be a plus to provide training on this subject to all ranks, possibly in
> basic training. We can never know too much about national security and how to preserve
> it."

> "Information protection needs to be installed in training for operators.
> Information attack and command and control warfare needs to be put in support officers
> curriculum (air operations 101 would be good too.)"

Two comments were received that were not in favor of training. They are listed
below:

> "I do not affect information warfare, information operations or information
> superiority. I do not think information warfare training would help me do my job better."

> "With all the requirements that we have to maintain and can barely keep up
> with, this would be one more thing that the majority of USAF personnel would get very
> little benefit at this time."

31

Ten respondents made comments that they had never received training or had never heard of IW or IO. Their comments are summarized below:

"I have never heard of information warfare training."

"All this information is new to me. The first time that I've seen it was on this survey. My answers to this survey were based solely on me reading the definitions now and re-reading them as I went along."

"I have no idea what any of this is, and I can't remember being told any of it."

"I have no idea what is all this about."

"Being a low ranking airman, I am not familiar with what this survey is asking."

"All of my questions are opinion since I've had no training in this area."

"I have received no training in this area."

"This info is new to me, and I haven't a clue what you're talking about."

"Being a young airman I do not know much about information warfare. I would like to learn more about information warfare. Due to my job on the flight line, and the systems I work on, the information might be valuable to me and my co-workers."

"I hope that this survey is as helpful to you as it was to me in making me aware of how little I really know about the preceding questions."

Summary of Analysis

Chapter IV has used descriptive statistics to reveal the basic results of the survey. Additional statistical analysis was used in determining how factors such as officer/enlisted, major command, TAFMS, and training affected the items measured. Training does appear to significantly raise individuals awareness of IW, IO, and related items.

Chapter V discusses what was learned about the research questions, identifies limitations of the research and survey, and provides observations regarding IW and IO awareness. It also discusses limitations of the study and provides suggestions for further research.

V. Discussion

Chapter V discusses the results of the survey as they pertain to the research questions. Chapter V also discusses limitations of the research and suggests further research.

Research Questions Discussion

Research Question 1: To what extent are AF members aware of the current AF definitions of information operations and information warfare? Over 60 percent of AF individuals indicated that they were aware of IO and IW concepts and definitions. Members were asked if they were aware of IO/IW, if they understood IO/IW, and if they thought the AF's definitions of IO/IW were useful. Given that the AF has recognized IW since 1995, a response rate of 60 percent suggests that AF officers and enlisted are getting the word. The AF first recognized IW in Cornerstones in 1995. The AF also stood up an information warfare squadron and the AF Information Warfare Center (AFIWC). The AF created IO and IW definitions in AFDD 1. The AF is also working on AFDD 2-5, Information Operations. The top management support of IO and IW does appear to be filtering down to the individuals.

Research Question 2: To what extent are AF members aware of how information operations and information warfare affect them? More than 65 percent of people believe IO affects their individual job, while 73 percent of people believe that IO affects their organization. Again, based on the time that individuals have been exposed to IO and IW concepts, these response rates suggest that the information is getting out and being heard. Given that 60 percent of people were aware of IO/IW concepts, response rates of 65 and

73 percent are very good. If people are aware of IO/IW then they may also be aware of how IO/IW affects them and their organization.

Research Question 3: To what extent are AF personnel aware of the differences between offensive and defensive information operations/information warfare? The survey results indicate this to be the least emphasized area. AFDD 2-5, Information Operations seems to be the best guidance for determining what is offensive versus defensive IO/IW. However, AFDD 2-5 is still in draft form and can not be officially used for guidance yet.

IO/IW defense is everyone's job. The AF does seem to emphasize information protection to everyone. Sixty-nine percent of people said that they were aware of the differences between offensive and defensive IO/IW. PSYOPs, military deception, and physical destruction were perceived mainly as offensive weapons. This may be somewhat true; however, for every offense there may be an equal defense. Physical destruction is not perceived as being part of IO/IW by many people. AFDD 2-5, Information Operations, does include physical destruction as part of information warfare. As long as these differences in awareness exist, more education on IO/IW is needed.

Research Question 4: To what extent are AF members aware of how Information Superiority links to information operations/information warfare? Approximately 80 percent of individuals indicated that they agreed with the survey statements on how IS links to IO/IW. The fact that information superiority is a core competency may be the reason why information superiority is more accepted than IO/IW in general. The AF has emphasized core competencies in documents such as AFDD 1. Individuals seem to understand that information superiority includes IO and IW. Perhaps by better linking IO

34

and IW to IS, more people will be aware of IO and IW and training could enforce the link between IS, IO and IW.

Research Question 5: To what extent have AF members been formally trained on information operations and information warfare and by what system? More than one-third of individuals indicated that they had received some form of training on IO/IW. A majority of those individuals received their training in-house. Professional military education (PME) accounted for a portion of those receiving IO/IW training. Different individuals felt different levels of training were necessary. Individuals' comments on the survey indicated that it behooves everyone to know the basics of IO and IW. IWAC may be the best method for educating and training those individuals who conduct in-house training or other forms of IO/IW training in the AF. This would give a basis to IO/IW training and may eliminate large differences in focus between various training. PME and basic training may be the method for educating the officer and enlisted troops on IO/IW. All enlisted go through basic training and officers go through the Reserve Officers Training Corps (ROTC), the Academy (USAFA), or Officer Training School (OTS). In-house training may be necessary for organizations that deal directly in IO/IW such as the information warfare squadron or AFIWC. However, all the training needs to be based in some core knowledge. IWAC could provide the core knowledge and centralization for disseminating IO/IW training throughout the AF.

Research Question 6: To what extent does information operations/information warfare training improve the awareness of information warfare in AF members? Responses confirm that training is important. Training raises the level of knowledge and awareness for a majority of the items measured in the survey including: IW awareness,

35

IO awareness, AFDD 1 awareness, IO affects on individual jobs and organizations, offensive/defensive IO/IW differences, and information superiority.

Overall Awareness Assessment

Given the AF focus on IO/IW since 1995, awareness levels appear to reflect a significant dissemination of knowledge in a short period of time. Training could be continued or increased if the AF wants to increase individuals' awareness of IO and IW concepts and definitions. Training through CADRE/IWAC, PME, and basic training appear to be a productive way to increase awareness levels to all members of the AF.

Limitations of Research

The research presented here has some limitations. Since no previous studies or surveys were found that measured IO/IW awareness, the survey used in this research is first-generation and was created entirely for this research. Therefore, the reliability of the survey has not been tested. This research presents a baseline of the current awareness levels. Further research is necessary to evaluate whether awareness levels are increasing or decreasing.

Another limitation of the research is the possibility of error in the measures. Respondents were asked for their opinion on how aware they felt they were. Respondent bias was possible. Individuals who were more aware of IO/IW could have been more likely to respond to the survey.

The final limitation of the research is the response rate. Overall, a response rate of 50 percent was desired. The final response rate was 27 percent, or almost half of the anticipated response rate. The implication of the response rate is that the survey results

may not be as representative of the AF population as desired. However, the response of 214 was enough to use parametric statistical analysis.

Further Research Suggestions

There are two main recommendations for further research. Given that this is the first study into IO/IW awareness levels, my main suggestion is to perform follow-up studies to confirm these findings and to measure changes in the IO/IW awareness levels. Repeated research will give an idea of how awareness levels are changing over time. The second suggestion for a further research is to measure the effectiveness of the various IO/IW training methods such as IWAC, PME, and basic training. This study would focus on the strengths and weaknesses in each method and attempt to standardize the training.

Summary

Information warfare and information operations are increasingly important as the AF relies more on information, computer, and telecommunications technologies. This research revealed that about sixty percent of AF individuals are aware of information warfare and information operations concepts and definitions. It also found that individuals with training are generally more aware of IO/IW concepts and definitions than individuals without training. If the AF requires a higher level of IO/IW awareness, this research suggests that providing additional training is likely to be effective.

Appendix A: Glossary of Terms and Acronyms

Unless otherwise noted, the source of all terms listed in this glossary is: Air Force Doctrine Document 1: Air Force Basic Doctrine.

Air superiority: That degree of dominance in the air battle of one force over another which permits the conduct of operations by the former and its related land, sea and air forces at a given time and place without prohibitive interference by the opposing force. (Joint Pub 1-02)

Core competency: The basic areas of expertise or the specialties that the Air Force brings to any activity across the spectrum of military operations whether as a single Service or in conjunction with the core competencies of other Services in joint operations. Core competencies represent both air and space power application theory and physical capability represented in a well-trained and equipped air force.

Deception: Those measures designed to mislead the enemy by manipulation, distortion, or falsification of evidence to induce him to react in a manner prejudicial to his interests. (Joint Pub 1-02)

Doctrine: Fundamental principles by which the military forces or elements thereof guide their actions in support of national objectives. It is authoritative but requires judgment in application.(JP 1-02)

Electronic warfare: Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. (Joint Pub 1-02)

Information attack: An activity taken to manipulate or destroy an adversary's information systems without visibly changing the physical entity within which it resides. (AFDD 2-5)

Information operations: Those actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO.

Information superiority: The ability to collect, control, exploit and defend information while denying an adversary the ability to do the same. See also information. (Joint Pub 1-02) [*The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same.*] {Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

Information warfare: Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while leveraging and defending one's own information, information-based processes, information systems, and computer-based networks. Also called IW. (Joint Pub 1-02) [*Information operations conducted during time of crisis or conflict to*

achieve or promote specific objectives over a specific adversary or adversaries.]
{Italicized definition in brackets applies only to the Air Force and is offered for clarity.}

Information: 1. Facts, data, or instructions in any medium or form. 2. The meaning that a human assigns to data by means of the known conventions used in their representation. (Joint Pub 1-02)

Information: Facts told or heard or discovered. (Oxford American Dictionary)

Military deception: Actions executed to deliberately mislead adversary military decision-makers as to friendly military capabilities, intentions, and operations, thereby causing the adversary to take specific actions (or inactions) that will contribute to the accomplishment of the friendly mission. (Joint Pub 1-02)

Operations security: A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a) Identify those actions that can be observed by adversary intelligence systems. b) Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c) Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. (Joint Pub 1-02)

Physical attack: The means to disrupt, damage, or destroy information systems through the conversion of stored energy into destructive power.

Psychological operations: Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. (Joint Pub 1-02)

ACC: Air Combat Command

ACOT: Advanced Communications-Information Officer Training

ACSC: Air Command and Staff College

AETC: Air Education and Training Command

AF: United States Air Force

AFCERT: Air Force Computer Emergency Reaction Team

AFDD: Air Force Doctrine Document

AFI: Air Force Instruction

AFIT: Air Force Institute of Technology

AFIWC: Air Force Information Warfare Center

AFMC: Air Force Materiel Command

AFPC: Air Force Personnel Center

AFSOC: Air Force Special Operations Command

AIA: Air Intelligence Agency

AMC: Air Mobility Command

ANOVA: Analysis of variance

BCOT: Basic Communications-Information Officer Training

CADRE: College of Aerospace Doctrine, Research, and Education

CGO: Company grade officer

COMPUSEC: Computer Security

EW: Electronic warfare

FGO: Field grade officer

HQ: Headquarters

IO: Information operations

IS: Information superiority

IW: Information warfare

IWAC: Information Warfare Applications Course

JCS: Joint Chiefs of Staff

JV: Joint Vision

MAJCOM: Major command

NCO: Non-commissioned officer

NDU: National Defense University

OPSEC: Operations Security

OTS: Officer Training School

PACAF: Pacific Air Forces

PSYOP: Psychological Operations

SATE: Security Awareness Training and Education

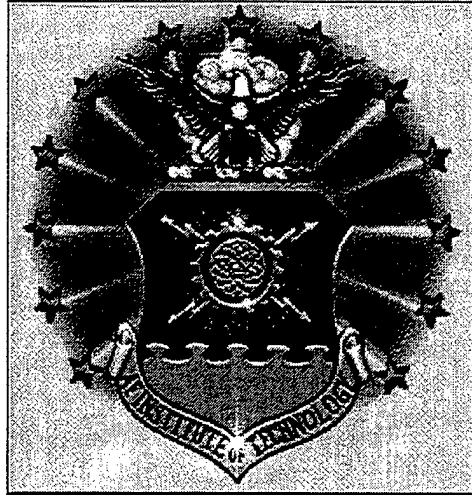SIWAC: Senior Information Warfare Applications Course

TAFMS: Total Active Federal Military Service

USAF: United States Air Force

USAFA: United States Air Force Academy

USAFE: United States Air Forces in Europe

AFIT SURVEY OF INFORMATION OPERATIONS/ INFORMATION WARFARE AWARENESS

USAF SCN 98-42

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY (AETC)
AIR FORCE INSTITUTE OF TECHNOLOGY

Information
About this Research Study

Description of the study: The purpose of this study is to measure the current awareness level of information operations and information warfare concepts in the U.S. Air Force.

How your responses will be used: The data collected will be analyzed to determine the current awareness level and those areas that may need additional attention in information warfare training.

Confidentiality of your responses: This information is being collected for research purposes only. All responses will be compiled into statistical information and no individual responses will be identified. No one in your unit, base, or MAJCOM will ever see your individual responses.

Survey Control Number (SCN): USAF SCN 98-42 (expires 31 December 1998).

Purpose: This survey is being conducted to collect demographic, and awareness data regarding information warfare and information operations. This data will be analyzed to determine the current Air Force information warfare and information operations awareness levels. The summary data will also be used as input to Air University's College of Aerospace Doctrine, Research and Education (CADRE) Information Warfare Application Course (IWAC).

Routine Use: Future information warfare training will draw upon the data collected and analyzed for this research. No analysis of individual responses will be conducted and ONLY members of the research team will be permitted to access the raw data. Reports summarizing trends in information warfare awareness may be published. *No individual will be identified to anyone outside of the research team.*

Response: Please respond to this survey within two weeks of receiving it or at your earliest convenience. Prompt survey response will assist with the associated research efforts.

Participation: Participation is voluntary. No adverse action will be taken against any member who does not participate in this survey or who does not complete any part of this survey.

Contact Information

If you have any questions, please feel free to contact me:

Captain Ryan D. Hollman
AFIT/LAL
2950 P Street
Wright-Patterson AFB, OH 45433-7765

email: rhollman@afit.af.mil
DSN: 785-7777 ext. 2146

INSTRUCTIONS

This questionnaire contains 32 main items. Please answer each item by circling the appropriate response on the questionnaire. If for any item you do not find a response that fits your situation exactly, use the one that is closest to the way you feel.

1. Your current rank is:

a) O-4 to O-6 Field Grade Officer
b) O-1 to O-3 Company Grade Officer
c) E-7 to E-9 Senior NCO
d) E-5 to E-6 NCO
e) E-1 to E-4 Airman
f) Civilian

2. How many years of Total Federal Active Military Service (TAFMS) have you completed (14 years 8 months should be recorded as 14 years)? _____

3. Your current Major Command (MAJCOM) is:

a) Air Combat Command (ACC)
b) Air Education and Training Command (AETC)
c) Air Force Materiel Command (AFMC)
d) Air Force Special Operations Command (AFSOC)
e) Air Force Space Command (AFSPC)
f) Air Mobility Command (AMC)
g) Pacific Air Forces (PACAF)
h) United States Air Forces in Europe (USAFE)
i) Other (including Direct Reporting Units and Forward Operating Agencies), please specify below:

_____

The following questions measure aspects of information operations/information warfare awareness.

Definitions: All definitions are from *Air Force Doctrine Document 1: Air Force Basic Doctrine*, Secretary of the Air Force, September 1997.

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

Information operations: Those actions taken to affect adversary information and information systems while defending one's own information and information systems. Also called IO.

Information superiority: The ability to collect, control, exploit and defend information while denying an adversary the ability to do the same.

4. I am aware of the concept of information warfare as defined by the Air Force.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

5. I understand the Air Force's definition of "information warfare."

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

6. The Air Force's definition of information warfare is useful.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

7. I have a different definition of information warfare from the Air Force's definition.

Yes   No

7a. If yes, what is your definition of information warfare?

_____

_____

_____

8. I am aware of the concept of information operations as defined by the Air Force.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

45

9. I understand the Air Force's definition of "information operations."

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

10. The Air Force's definition of information operations is useful.

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

11. I have a different definition of information operations from the Air Force's definition.

Yes   No

11a. If yes, what is your definition of information operations?

_____

_____

12. I am familiar with the information contained in Air Force Doctrine Document 1 (AFDD 1).

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

13. Information warfare is different from information operations.

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

14. Information warfare contributes to information superiority.

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

15. Information operations contribute to information superiority.

Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree

The next set of questions deals with how information operations and information warfare affect AF members.

According to AFDD 1, information warfare is information operations conducted during time of conflict or crisis to achieve or promote specific objectives over a specific adversary or adversaries. Therefore, information warfare is a subset of information operations. Questions 16-28 refer to information operations; please keep in mind that this includes information warfare as defined above.

16. My job is directly affected by information operations.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

17. My organization is directly affected by information operations.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

The next set of questions deals with offensive and defensive information operations/information warfare.

18. I am aware of the differences between offensive and defensive information operations.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

19. Offensive information operations include psychological operations.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

20. Offensive information operations include electronic warfare.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

21. Offensive information operations include military deception.

| Strongly Disagree | Disagree | Neither Agree Nor Disagree | Agree | Strongly Agree |

22. Offensive information operations include physical destruction.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

23. Offensive information operations include information attack.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

24. Defensive information operations include psychological operations.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

25. Defensive information operations include electronic warfare.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

26. Defensive information operations include military deception.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

27. Defensive information operations include physical destruction.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

28. Defensive information operations include information attack.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

The next set of questions deals with the relationship between information superiority and information warfare.

29. I am aware of the concept of information superiority as defined by the Air Force.

Strongly   Disagree   Neither Agree   Agree   Strongly
Disagree   Nor Disagree   Agree

30. Information operations support information superiority.

| Strongly | Disagree | Neither Agree | Agree | Strongly |
| Disagree | | Nor Disagree | | Agree |

31. Information superiority is necessary for air superiority.

| Strongly | Disagree | Neither Agree | Agree | Strongly |
| Disagree | | Nor Disagree | | Agree |

The last set of questions deals with information warfare training.

32. I have had some form of formal information warfare training.

Yes   No

32a. If yes, how did you receive information warfare training?

a) Air Force Institute of Technology's (AFIT) Information Warfare course
b) College of Aerospace Doctrine, Research and Education (CADRE)/ Information Warfare Applications Course (IWAC)
c) National Defense University's (NDU) Information Warfare course
d) U.S. Air Force Academy's (USAFA) Information Warfare course
e) Unit/organizational in-house training
f) Other, please specify _____

32b. If no, it would be valuable for me to receive information warfare training.

| Strongly | Disagree | Neither Agree | Agree | Strongly |
| Disagree | | Nor Disagree | | Agree |

COMMENTS - Please write any comments below.

_____

_____

_____

_____

_____

_____

49

Appendix C: Survey Data

Descriptive Statistics

	N	MISSING	LO 95% CI	MEAN	UP 95% CI	SD	MINIMUM	MAXIMUM
TAFMS	213	1	10.05	10.977	11.903	6.8601	0	27
Question 4	213	1	3.7163	3.8263	3.9363	0.8143	1	5
Question 5	213	1	3.8306	3.9296	4.0286	0.7331	1	5
Question 6	213	1	3.6328	3.723	3.8133	0.6682	2	5
Question 7	211	3	8.81E-03	0.0332	0.0575	0.1795	0	1
Question 8	212	2	3.6163	3.7311	3.8459	0.8478	1	5
Question 9	214	0	3.7672	3.8645	3.9618	0.7221	1	5
Question 10	214	0	3.5743	3.6682	3.7621	0.6969	1	5
Question 11	210	4	-1.90E-03	0.0143	0.0305	0.1189	0	1
Question 12	213	1	2.6702	2.8122	2.9543	1.0517	1	5
Question 13	213	1	3.2636	3.3803	3.497	0.8638	1	5
Question 14	213	1	3.7801	3.8826	3.9851	0.7588	1	5
Question 15	213	1	3.7779	3.8732	3.9686	0.7057	1	5
Question 16	209	5	3.4573	3.5837	3.7102	0.9271	1	5
Question 17	208	6	3.6245	3.7452	3.8659	0.8833	1	5
Question 18	208	6	3.5123	3.625	3.7377	0.8246	1	5
Question 19	208	6	3.596	3.6875	3.779	0.6692	1	5
Question 20	208	6	3.6444	3.7404	3.8363	0.7019	2	5
Question 21	207	7	3.6802	3.7681	3.8561	0.6419	2	5
Question 22	209	5	3.3128	3.4306	3.5484	0.8639	1	5
Question 23	210	4	3.6395	3.7286	3.8176	0.6545	2	5
Question 24	210	4	3.3136	3.4238	3.5341	0.8105	1	5
Question 25	209	5	3.596	3.689	3.782	0.6821	2	5
Question 26	210	4	3.7129	3.8	3.8871	0.64	2	5
Question 27	210	4	3.1422	3.2667	3.3912	0.9152	1	5
Question 28	210	4	3.0887	3.2048	3.3209	0.8534	2	5
Question 29	208	6	3.5147	3.625	3.7353	0.8068	1	5
Question 30	211	3	3.7487	3.8341	3.9195	0.6294	1	5
Question 31	211	3	3.7163	3.8294	3.9425	0.8334	1	5
Question 32	212	2	0.2889	0.3538	0.4187	0.4793	0	1
Question 32b	155	59	3.4438	3.5871	3.7304	0.903	1	5

TAFMS Frequency Distribution

YEARS	FREQ	PERCENT
0	6	2.8
1	12	5.6
2	17	8
3	12	5.6
4	3	1.4
5	4	1.9
6	15	7
7	6	2.8
8	15	7
9	4	1.9
10	5	2.3
11	8	3.8
12	15	7
13	2	0.9
14	11	5.2
15	11	5.2
16	9	4.2
17	14	6.6
18	6	2.8
19	17	8
20	9	4.2
22	4	1.9
23	4	1.9
24	2	0.9
25	1	0.5
27	1	0.5
TOTAL	213	100

Frequency Distribution of Agree/Disagree Questions

	Strongly Disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree	TOTAL
Question 4	3	19	17	147	27	213
Question 5	1	15	14	151	32	213
Question 6	0	9	58	129	17	213
Question 8	3	24	22	141	22	212
Question 9	1	14	24	149	26	214
Question 10	1	11	60	128	14	214
Question 12	16	87	37	67	6	213
Question 13	1	44	48	113	7	213
Question 14	2	12	27	140	32	213
Question 15	2	7	35	141	28	213
Question 16	5	27	40	115	22	209
Question 17	5	17	33	124	29	208
Question 18	5	18	40	132	13	208
Question 19	1	5	68	118	16	208
Question 20	0	12	49	128	19	208
Question 21	0	8	48	135	16	207
Question 22	2	32	63	98	14	209
Question 23	0	8	57	129	16	210
Question 24	2	27	71	100	10	210
Question 25	0	14	49	134	12	209
Question 26	0	7	47	137	19	210
Question 27	3	48	59	90	10	210
Question 28	0	52	70	81	7	210
Question 29	5	17	40	135	11	208
Question 30	2	4	38	150	17	211
Question 31	1	13	49	106	42	211
Question 32b	3	16	42	75	19	155

Bibliography

1. Aldrich, Richard W. (Maj, USAF). "The International Legal Implications of Information Warfare". Airpower Journal, 10: 3:99-110. Fall 1996.

2. Armstrong, George (Colonel, USAF). Professor, Joint Command, Control and Information Warfare School, Armed Forces Staff College, Norfolk VA. Telephone interview. 21 April 1998.

3. Becker, John D. (Lieutenant Colonel, USAF). "Re: IW Research." Electronic Message. 2208Z. 23 April 1998.

4. Cooper, Donald R. and C. William Emory. Business Research Methods (Fifth Edition). United States of America: The McGraw-Hill Companies, 1995.

5. Department of the Air Force. AFI 36-2601: Air Force Personnel Survey Program. http://afpubs.hq.af.mil/elec-products/pubs-pages/36-pubs.html. 1 February 1996.

6. Department of the Air Force. Air Force Basic Doctrine. Washington. September 1997. (AFDD 1).

7. Department of the Air Force. Air Force Information Operations (IO): A Snapshot. Washington. 1996.

8. Department of the Air Force. Cornerstones of Information Warfare. Washington. 1995.

9. Department of the Air Force. Information Operations. December 1997. (AFDD 2-5, Final draft).

10. Ehrlich, Eugene and others. Oxford American Dictionary. New York: Oxford University Press. 1980.

11. Fogelman, Ronald R. (USAF Chief of Staff). "Information Operations: The Fifth Dimension of Warfare." Defense Issues: 10, 47: http://www.defenselink.mil/pubs/di95/di1047.html. 25 April 1995.

12. Gumahad II, Arsenio T. (Lieutenant Colonel, USAF). "The Profession of Arms in the Information Age." JFQ, 14-20. Spring 1997.

13. Hogue, Preston B. (Civilian, USAF). "RE: AF IW Research." Electronic Message. 2045Z. 13 April 1998.

14. Information Warfare Division, College of Aerospace Doctrine, Research, and Education. Information Warfare Reference Disk. Maxwell AFB AL. 6 March 1998.

15. Joint Warfighting Center. Commander. Concept for Future Joint Operations: Expanding Joint Vision 2010. Fort Monroe VA. May 1997.

16. Kuehl, Daniel. "Educating the DOD About Information Warfare: Is the Glass Half Full, or Half Empty?" Electronic Message Attachment. 13 April 1998.

17. Kuehl, Daniel. "RE: IW Thesis Research." Electronic Message. 1844Z, 13 April 1998.

18. Kuehl, Daniel. Senior Fellow, School of Information Warfare and Strategy, National Defense University, Washington. Telephone interview. 13 April 1998.

19. Levien, Fred. Chairperson, Information Warfare / Information Operations Academic Group, Naval Postgraduate School, Monterey CA. Telephone interview. 10 May 1998.

20. Libicki, Martin C. Defending Cyberspace and Other Metaphors. Washington, Institute for National Strategic Studies, National Defense University. Washington. February 1997.

21. Libicki, Martin C. Senior Fellow, Institute for National Strategic Studies, National Defense University, Washington. Telephone interview. 13 April 1998.

22. Libicki, Martin C. What Is Information Warfare? Institute for National Strategic Studies, National Defense University. Washington. August 1995. http://www.ndu.edu/ndu/inss/insshp.html, 20 June 1997.

23. McKenna, Pat (TSgt, USAF). "Info Warriors: Battling for data dominance in the fifth dimension." Airman, 40, 9:27-31. September 1996.

24. Pearce, Thomas (Capt, USAF). Air Force Information Warfare Center, Kelly AFB TX. Telephone interview. 13 April 1998.

25. Peifer, Kenneth V. An Analysis of Unclassified Current and Pending Air Force Information Warfare and Information Operations Doctrine and Policy. MS thesis, AFIT/GIR/LAS/97D-10. Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, December 1997 (AD-A340379).

26. President's Commission on Critical Infrastructure Protection. "PCCIP Report Summary." WWWeb, http://www.pccip.gov/summary.html. 17 November 1997.

27. Sneakers. Prod. Walter F. Parkes and Lawrence Lasker. Universal Studios. 1992.

28. Steel, Robert P. Class lecture, ORSC 661, Making Sense of Research Data. Department of Graduate Logistics Management, Graduate School of Logistics and Acquisition Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, Spring 1998.

29. Thrasher, Roger D. (Captain, USAF). <u>Information Warfare: Implications for Forging the Tools</u>. MS thesis, Naval Postgraduate School, Monterey CA, June 1996 (AD-A311887).

30. Tzu, Sun (Griffith, Samuel B., trans.) <u>The Art of War</u>. New York: Oxford University Press. 1963.

31. United States. Chairman of the Joint Chiefs of Staff. <u>Joint Vision 2010: America's Military Preparing for Tomorrow</u>. Washington. 1995.

32. Wicks, Robert (Major, USAF). Chairman, Information Warfare Applications Course, College of Aerospace Doctrine, Research, and Education, Air University, Maxwell AFB AL. Personal interview. 16 January 1998.

<u>Vita</u>

Captain Ryan D. Hollman was born and raised in Wisner, Nebraska. He graduated from Wisner-Pilger High School in Wisner, Nebraska in May 1989. He received a four-year Air Force Reserve Officer Training Corps scholarship to study computer science. He earned a Bachelor of Science degree in Computer Science from Iowa State University and was commissioned from the Air Force Reserve Officer Training Corps program in December 1993.

As a Second Lieutenant, Ryan Hollman entered active duty in May 1994. He attended the Basic Officers Communications-Computer Training, BCOT, at Keesler AFB, Mississippi, and graduated in September 1994.

His first assignment was as Team Leader, Database Access Management at the Air Force Global Weather Center, Offutt AFB, Nebraska. In May of 1996, he transferred to the Project Management branch as a Software Project Manager. His greatest accomplishment was the successful implementation of a three million-dollar mainframe system for satellite weather processing.

He entered the Air Force Institute of Technology's Graduate Information Resource Management program at Wright-Patterson AFB, Ohio in March 1997 and graduated in September 1998. Captain Hollman was assigned to the Air Force Communications Agency (AFCA) at Scott AFB, Illinois following graduation.

Permanent Address: ███████████████

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 1998	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE
A DESCRIPTIVE STUDY OF INFORMATION OPERATIONS AND INFORMATION WARFARE AWARENESS IN THE UNITED STATES AIR FORCE

5. FUNDING NUMBERS

6. AUTHOR(S)

Captain Ryan D. Hollman

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
2950 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/LAS/98S-5

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
CADRE/WSW/IWAC
625 Chennault Circle
Maxwell AFB, AL 36112

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 Words)

Information has always been important in military affairs, conflicts, and wars. Information warfare is an important new concept that is emphasized by the significance of computer and information technology. The United States Air Force has educated and trained individuals in information warfare since recognizing the importance of information warfare in 1995. The Air Force Information Warfare Center and the information warfare squadron were also created to address information warfare concerns. Information warfare is important to the entire Air Force. How familiar are Air Force people generally in information warfare? This thesis addresses awareness of information warfare and information operations concepts. Despite the amount of focus, training, and education, it was unknown how aware individuals were concerning information warfare and information operations. This thesis surveyed eight hundred officers and enlisted personnel with a response rate of 214 to determine the baseline of information warfare awareness.

Approximately sixty percent of the respondents indicated that they were aware of information warfare. Also, individuals who received information warfare training responded higher than individuals without training. This is the first study in information warfare and information operations awareness. Additional research is needed to determine how the awareness levels are changing and the effectiveness of the training.

14. Subject Terms
Information, Warfare, Operations, Awareness, Electronic warfare

15. NUMBER OF PAGES
68

16. PRICE CODE

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

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project?   a. Yes   b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?

a. Yes   b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years_____ $_____

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly   b. Significant   c. Slightly   d. Of No
   Significant   Significant   Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

_____   _____
Name and Grade   Organization

_____   _____
Position or Title   Address