THE EFFECT OF EXTERNAL SAFEGUARDS ON HUMAN-INFORMATION SYSTEM TRUST IN AN INFORMATION WARFARE ENVIRONMENT

THESIS

Gregory S. Fields, Captain, USAF

AFIT/GIR/ENV/01M-07

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

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

AFIT/GIR/ENV/01M-07

THE EFFECTS OF EXTERNAL SAFEGUARDS ON HUMAN-INFORMATION SYSTEM TRUST IN AN INFORMATION WARFARE DOMAIN

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

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

Gregory S. Fields, B.S.

Captain, USAF

March 2001

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT/GIR/ENV/01M-07

THE EFFECTS OF EXTERNAL SAFEGUARDS ON HUMAN-INFORMATION SYSTEM TRUST IN AN INFORMATION WARFARE ENVIRONMENT

Gregory S. Fields, B.S.
Captain, USAF

Approved:

David P. Biros (Chairman)	9 Feb 01 date
Michael G. Morris (Member)	9FEB 01 date
Paul Thurston (Member)	9Feb01 date

Acknowledgments

I would like to express my sincere appreciation to my classmates and everyone else who helped me over the past year and a half. I especially want to thank Major Biros, my thesis committee chairman, for giving me direction and guidance throughout the research process. I would also like to thank Major Morris for his consul and ability to transform my writing style into something that at least resembles an academic paper. Thanks also to Major Thurston for his expert statistical advise and for not giving up on my slow grasp of that subject. Of course I would also like to thank my sponsors, the Air Force Office of Scientific Research and the Air Force Research Laboratory, Human Effectiveness Branch at Brooks AFB, TX. Without their generosity in both time and money, this research project would not have been possible. A special thanks to Dr. Elliot Entin, Dr. Linda Elliot, Dr. D. Harrison McKnight, and Dr. Sam Schiflett for their assistance, advise, and encouragement. Additionally, I would like to thank Colonel Kennedy and the men and women of the 552nd AWACS Group, Tinker AFB, OK and the Air War College, Maxwell AFB, AL. Finally and most importantly, I would like to thank my family for their love and support. To my two daughters, [redacted] and [redacted], thanks for reminding me to take time out to play and have fun. To my wife, [redacted], thank you for picking up the extra workload around the house and for taking care of me and the girls. Your love and support sustained me through the stress and anxiety of the past year and a half .

Gregory S. Fields

Table of Contents

Page

Acknowledgments iv

List of Figures ix

List of Tables x

Abstract xi

I. INTRODUCTION 1
Background 1
Research Applicability to the United States Air Force 3
Problem Statement and Purpose of Research 4
Summary 4
Thesis Organization 5

II. LITERATURE REVIEW 6
Introduction 6
Decision Making Theories 8
Command and Control 13
Information Warfare 14
Theories of Trust 17
Applicability to Human-Information System trust 29
Research Hypotheses 29
Summary 35

III. METHODOLOGY 37
Overview 37
Experimental Design 37
Pilot Study 41
Subjects 42
Equipment and Facilities 42
Tasks and Procedures 43
Experiment Manipulations 46
Hypothesis Measures 49
Survey Design and Validation 53
Data Analysis 53
Summary 54

IV. ANALYSIS OF DATA 55
Data Analysis 55

Relationship Between Disposition to trust and Situational decision to trust (H1) 57
Relationship Between Disposition to trust and Trusting behavior (H2)..... 57
Relationship Between Situational decision to trust and Trusting behavior (H3)..... 58
Effect of External Safeguards on Trusting behavior (H4) 58
Effect of Information Warfare on Trusting behavior (H5) 59
Conclusion 59

V. METHODOLOGY 61
(Experiment 2) 61
Overview..... 61
Experimental Design..... 61
Pilot Study..... 65
Subjects..... 66
Equipment and Facilities..... 66
Tasks and Procedures..... 67
Experiment Manipulations..... 69
Hypothesis Measures 72
Survey Design..... 76
Data Analysis..... 76
Summary..... 77

VI. ANALYSIS OF DATA..... 78
Data Analysis..... 78
Relationship Between Disposition to trust and Situational decision to trust (H1) 80
Relationship Between Disposition to trust and Trusting behavior (H2)..... 80
Relationship Between Situational decision to trust and Trusting behavior (H3)..... 81
Effect of External Safeguards on Trusting behavior (H4) 81
Effect of Information Warfare on Trusting behavior (H5) 82
Conclusion 82

VII. FINDINGS..... 83
Introduction..... 83
Dispositional trust and situational decision to trust are positively correlated (H1)..... 83
Disposition to trust will have a positive effect on trusting behavior (H2)..... 84
Situational decision to trust will positively affect trusting behavior (H3)..... 84
External safeguards have a positive effect on trusting behavior (H4) 85
Information warfare has a negative effect on trusting behavior (H5)..... 86
Research Finding Overview..... 87
Research Limitations 88
Implications..... 89
Recommendations for Future Research..... 90
Summary..... 91

Appendix 1: Air Space Boundary Layout 94

Appendix 2: IW Threat Message 95

Appendix 3: Scenario Brief 96

Appendix 4: Simulation Scoring System 98

Appendix 5: Multiple Choice Test 99

Appendix 6: Experiment Room Layout 101

Appendix 7: Randomized Block Design 102

Appendix 8: Subject Consent Form 104

Appendix 9: Biometric Data Form 105

Appendix 10: Training Presentation 106

Appendix 11: Pre-Test Survey 113

Appendix 12: Post-Test Survey 115

Appendix 13: Air Space Boundary 118

Appendix 14: IW Threat Message 119

Appendix 15: Scenario Brief 120

Appendix 16: Simulation Scoring System 122

Appendix 17: Randomized Block Design 123

Appendix 18: Subject Consent Form 125

Appendix 19: Biometric Data Form 126

Appendix 20: Survey One (Dispositional Trust) 127

Appendix 21: Survey Two (Situational Decision to Trust) 128

Appendix 22: Training Presentation 129

Appendix 23: Survey Three (Trusting Belief) 136

Appendix 24: Fratricide Warning 137

Bibliography 138

Vita.....145

List of Figures

Figure Page

1. OODA Model.....11
2. Man-Machine Model of Trust.....20
3. Theory of Reasoned Action model 25
4. McKnight's Model of Trust.....26
5. Adapted Model of Trust.....29
6. Group Configurations 38
7. Experimental Time-line 43
8. Adapted Model of Trust.....50
9. Descriptive Statistics of Trusting behavior Data 56
10. Group Configurations 62
11. Experimental Time-line (Experiment 2).....67
12. Adapted Model of Trust.....72
13. Trusting Behavior Normality Analysis.....79

List of Tables

Table Page

1. List of NDM Factors 10
2. Definition of Constructs 31
3. Item Clusters 52
4. Descriptive Statistics and Intercorrelations of Independent Variables 57
5. Log-linear Regression Analysis Summary 58
6. Item Clusters 74
7. Descriptive Statistics and Intercorrelations of Independent Variables 80
8. Regression Analysis Summary 81

AFIT/GIR/ENV/01M-07

Abstract

This research looks at how human trust in an information system is influenced by external safeguards in an Information Warfare (IW) domain. The military command and control environment requires decision-makers to make tactical judgments based on complex and conflicting information received from various sources such as automated information systems. Information systems are relied upon in command and control environments to provide fast and reliable information to the decision-makers. The degree of reliance placed in these systems by the decision-makers suggests a significant level of trust. Understanding this trust relationship and what effects it is the focus of this study. A model is proposed that predicts behavior associated with human trust in information systems. It is hypothesized that a decision-maker's belief in the effectiveness of external safeguards will positively influence a decision-maker's trusting behavior. Likewise, the presence of an Information Warfare attack will have a negative affect a decision-maker's trusting behavior. Two experiments were conducted in which the perceived effectiveness of external safeguards and the information provided by an information system were manipulated in order to test the hypotheses presented in this study. The findings from both experiments suggest that a person's trust computers in specific situations are useful in predicting trusting behavior, external safeguards have a negative effect on trusting behavior, and that Information Warfare attacks have no effect on trusting behavior.

THE EFFECT OF EXTERNAL SAFEGUARDS ON HUMAN-INFORMATION SYSTEM TRUST IN AN INFORMATION WARFARE ENVIRONMENT

I. INTRODUCTION

Background

Historians will likely reflect on the Twentieth Century as an era of unprecedented advancements in science and technology. Of these advancements, perhaps none has transfigured our society as profoundly as the "information technology revolution" (Halal, 1992). Information technology has transformed society socially, economically, and politically (Sheridan, 2000). An example of this transformation is the conversion of the United States economy from a post-World War II industrial based economy to the current information services based economy (Gray, 1999). By the last half of the Twentieth Century, information technologies have become the primary means by which information is processed and exchanged (Halal, 1992, McConnell, 1996).

Not only are information technologies used as a means of processing and exchanging information, but also they are increasingly used and relied upon to control and operate critical functions in society. This growing trend has generated sufficient interest by researchers to examine the behavior of people who rely on these information

systems (Biros, 1998; Muir, 1996; Morray and Lee 1992; Mosier, Stitka, and Burdick, 2000, Sheridan and Hennessy, 1984, Bisantz, Llina, Seong, Finger, and Jian 2000). A recent issue of a leading information technology journal, Communications of the ACM, devoted the entire issue to trust in information systems (Friedman, Kahn, and Howe, 2000; Olson and Olson, 2000; Resnick, Zeckhauser, Friedman, and Kuwabara, 2000; Cassell and Bickmore, 2000; Shneiderman, 2000; Uslaner, 2000).

Most of the current research efforts have attempted to apply human-human relationship models, such as trust, to the human-information system relationship (Biros, 1998; Muir, 1996; Morray and Lee 1992). While these researchers have found some evidence to support the idea that humans trust information systems in the same way humans trust other humans, there are enough significant differences to continue this line of research.

Unfortunately, this stream of research is somewhat disjoint. So many different definitions and facets of trust have been used in this area of study that it becomes difficult to adequately compare the findings from existing research. In fact, one of the leading trust theorists described this situation as a "conceptual morass" (Barber, 1983: 1). While there is no one generally accepted definition of trust, there are some commonalties among these definitions. For example, trust is often defined in terms of a behavior of reliance (McKnight and Chervany, 1999). This is consistent with Webster's Third new International Dictionary which defines trust as an "assumed reliance on some person or thing; a confident dependence on the character, ability, strength, or truth of someone or something" (Gove, 1981).

Mayer, Davis, & Schoorman (1995) suggest that, as a person becomes reliant (through the act of bestowing trust) on another person, the trustor becomes vulnerable to the trustee. Carrying this concept to the human-information system trust relationship, it suggests that people become vulnerable to potentially negative consequences because of their trust in these systems (Bonoma, 1975, Giffin, 1967). This vulnerability becomes even greater as society continues to rely on computer technology, not only for simple automation, but also as critical and complex information systems (DeSanctis and Poole, 1994).

Research Applicability to the United States Air Force

The United States Air Force, like the other branches of the military, has become increasingly reliant upon complex information systems. A 1996 article in the Washington Post illustrates the degree of this reliance:

> the American military is the most information-dependent force in the world. It uses computers to help design weapons, guide missiles, pay soldiers, manage medical supplies, write memos, control radio networks, train tank crews, mobilize reservists, issue press releases, find spare parts and even suggest tactics to combat commanders (Washington Post, 16 July 1996).

Consequently, the Air Force has allowed itself to become vulnerable due to its heavy reliance on information systems. In response to this perceived vulnerability, the Secretary of the Air Force and Air Force Chief of Staff called for a change to Air Force operational strategy and tactics in order to ensure the Air Force gains and maintains information superiority (Cornerstones of Information Warfare, 1996).

Part of establishing information superiority involves maintaining an effective defense against adversarial attacks that are directed against critical information systems

(Cornerstones of Information Warfare, 1996). A great deal of work to mitigate the risk of this type of attack has focused on the development of effective physical barriers and increased security awareness training for its personnel (Mayer, 2000). Despite these efforts, unauthorized intrusions into Air Force information systems continue to occur as illustrated by a recent network security test conducted by the Air Force Information Warfare Center (IWC). The IWC noted that of the networks tested "46 percent were successfully accessed, and IWC operators were able to obtain total control of 28 percent of the systems" (as quoted in Biros, 1998). Examples and theories of the type of damage caused by network attacks is abundant in both news reports and research studies (Van Cleave, 1997; Roman, 1999; Mayer, 2000; Whitehead, 1999). Unfortunately, little is known about the behavioral effect these attacks have on the decision-maker who is reliant upon these systems.

Problem Statement and Purpose of Research

Understanding the factors that influence a person's trust in information systems in an adversarial environment is important, not only for the United States Air Force, but for any organization that relies upon information systems. This study examines some of the variables that may influence a person's trust in information systems and proposes a theoretical framework to study the effects of these variables on human behavior in a military command and control environment..

Summary

The explosive reliance on information systems has brought both benefits in terms of increased communication and productivity, and liabilities in terms of increased

vulnerabilities to deception. Despite the potential consequences of these vulnerabilities, information technologies continue to be relied upon to perform increasingly critical functions in society. Given the United States Air Force's reliance on information systems as strategic and tactical decision-making tools, it is crucial to understand the effects of trust in an adversarial environment.

Thesis Organization

The following chapters present support for a conceptual framework that will be used to observe some variables that may influence a person's trusting behavior. Chapter II provides a literature review of the body of work in decision-making, information warfare, and trust. A series of hypotheses is also offered that will be tested in two empirical experiments. Chapter III explains the experimental and methodological framework for the first experiment used to test the hypotheses. Chapter IV presents the statistical analysis of the data collected from the first experiment. Chapter V explains the experimental and methodological framework for the second experiment and Chapter VI presents the statistical analysis of the data collected from this experiment. Finally, Chapter VII synthesizes and compares the analysis of both experiments and presents the research findings and conclusions.

II. LITERATURE REVIEW

Introduction

Marshall McLuhan is often remembered for his prediction that all societies will one day blend together into a "global village" as a result of advances in information technology (McLuhan 1989). In many ways, McLuhan's predictions have become a reality. Information technology has transformed societies socially, economically, and politically (Sheridan, 2000). Over the past two decades, the extent of this transformation has been profound, both in terms of the extent to which information is shared and in terms of the extent to which information technology is relied upon to perform critical tasks.

The term "information technology" is often vaguely defined. DeSanctis and Poole define advanced information technologies (AIT) as those "technologies that enable multi-party participation in organizational activities through sophisticated information management" (DeSanctis and Poole, 1994: 121). These technologies include electronic mail, electronic data transfer systems, and decision support systems (Biros, 1998). Information systems are defined in this study as any AIT artifact that provides information to decision-makers.

Understanding why some societies have become so dependent upon information systems is the topic of debate among modern philosophers (Kellner, 1997; Borgmann, 1992; Wickens, 1999). Some argue the use and reliance upon information systems is simply a natural progression of a capitalistic society (Kellner, 1997). This school of

thought argues that monetary gain is the underlying driver of information systems. Others believe that information systems are an enabler by which society reorganizes itself (Borgmann, 1992). For instance, the emergence and use of electronic mail and chat rooms extend social networks to an extent not otherwise possible before the advent of information systems (Kellner, 1997). Still others argue the reliance on information systems is a solution to the inherent complexities of modern life (Parasuraman, 1987; Wickens, 1999). Examples of these complexities include control of nuclear power plants, air traffic control systems, and military operations. These complex systems require information systems to help people synthesize and analyze huge amounts of information in order to efficiently and effectively manage them. While pondering the cause for the explosive use of information systems in society is of interest to philosophers, exploring the behavioral effects associated with the use of these systems is also of interest to researchers.

This chapter explores the human-information system trust relationship and examines how attitudes and events may effect this relationship. It begins by reviewing pertinent literature related to this research and then presents a theoretical framework within which this issue will be explored. Theories reviewed include decision-making (Simons, 1957; Orasanu and Connolly, 1993), information warfare (McCornack, Levine, Morrison, and Lapinski, 1996; Whitehead, 1997; Biros, 1998), and trust (Zuboff, 1988; Muir, 1994; Mosier, Skitka and Burdick, 2000, McKnight and Chervany, 1999). Finally, hypotheses will be presented that relate to the influence information warfare and external safeguards have on the behavior of people who rely on information systems to aid in decision-making.

Decision Making Theories

In order to understand how humans trust information systems in a command and control environment, it is important to first understand how those information systems are used by the military commander. In modern military command and control centers, military commanders use a wide variety of information systems to synthesize and display information about the battle space (Klein, 1988; Roman, 1999). This information is primarily used by the military commander to make decisions. Therefore, a review of literature on decision-making was performed in order to understand how decisions are made and what types of things could effect the decision-maker.

Decision-making theories are rich and span across various academic disciplines (Simon, 1957; March and Simon, 1958; Hall, 1996; Zey, 1992). For instance, theories and models of decision-making were found in organizational behavior, management, strategy, and cognitive psychology. Despite this, a review of decision making research found that these theories and models fall into one of two main schools of thought: Rational Choice and Naturalistic Decision Making.

Rational Choice

Most modern theories dealing with decision-making begin with a theoretical model called the Rational Choice model. (Simon, 1957; Hall, 1996). The Rational Choice model is divided into three areas: certainty, risk, and uncertainty.

The certainty area is sometimes referred to as the economic man model. The economic man "…is characterized by the following: acting only in his self-interest, possessing full information about the decision problem, knowing all the possible

solutions from which he has to choose as well as the consequences of each solution, seeking to maximize utility, having the ability to rank alternatives in order of likelihood of maximizing outcomes" (Zey, 1992: 11). However, March and Simon (1958) acknowledge some difficulties with this area of classical decision-making theory. They point out that classical decision-making theories based on certainty make assumptions that, often, do not exist in reality. For instance, March and Simon (1958) recognize that these theories hinge upon the assumption that decision-makers know *all* possible information required to determine *all* possible outcomes for a decision and are able to develop an *optimal* order for these outcomes. However, in reality most decisions are made with uncertainty. Simon (1957) refers to this area of decision-making as "bounded rationality."

Simon (1959) suggests that in situations where uncertainty exists, a behavior called "satisficing" may occur. Satisficing is perhaps best defined by the analogy given by Simon (1959) where he describes a man searching for the sharpest needle, of many, in a haystack. Instead of trying to find all of the needles and comparing each of them to one another in order to see which is the sharpest, the man stops after finding a needle that is sufficiently sharp. Most modern decision-making research is grounded in bounded-rationality. One such growing area of decision-making research is Naturalistic Decision Making.

Naturalistic Decision Making

In the mid-1980s, a decision-making paradigm was proposed to explain how decision-making occurs in a bounded rationality context, or more simply in *uncertainty*.

This paradigm is referred to as Naturalistic Decision-Making (Orasanu and Connolly, 1993).

The Naturalistic Decision-Making movement began slowly, but has recently gained momentum and wider acceptance among serious researchers (Cannon-Bowers, Salas, and Grossman, 1991). This growing acceptance is due largely for the need to understand decision making as it occurs in a naturalistic setting by the actual people who make the decisions. This growing need is due, in part, to the increased complexities of modern society.

Naturalistic Decision Making is identified by eight factors that typify the naturalistic environment (See Table 1). In addition to these factors, Cannon-Bower,

Table 1. List of NDM Factors from Cannon-Bowers, Salas, and Pruitt, 1996

Eight Factors of Naturalistic Environment
• ill-structured problems • uncertain, dynamic environments • shifting, ill-defined, or competing goals • multiple event-feedback loops • time constraints • high stakes • multiple players • organizational norms and goals that must be balanced against the decision makers' personal choice

Salas, and Pruitt (1996) offer some additional factors that define decision-making in a naturalistic environment. One of these additional factors is "Multiple event feedback

loops" (Cannon-Bowers, Salas, and Pruitt, 1996). They propose that most decisions are "temporally dependent, ongoing series, with the outcome of iterative decisions affecting subsequent decisions" (Cannon-Bowers, Salas, and Pruitt, 1996: 199). This concept of a temporally dependent decision-making cycle supports a similar, however somewhat simpler decision-making model that was offered to explain how military commanders make decision in an adversarial environment.

Observation, Orientation Decision, Action (OODA) Loop Theory

The OODA Loop model (see Figure 4 below) proposed by Air Force Colonel John Boyd (1987) describes the decision-making process of military commanders in C2

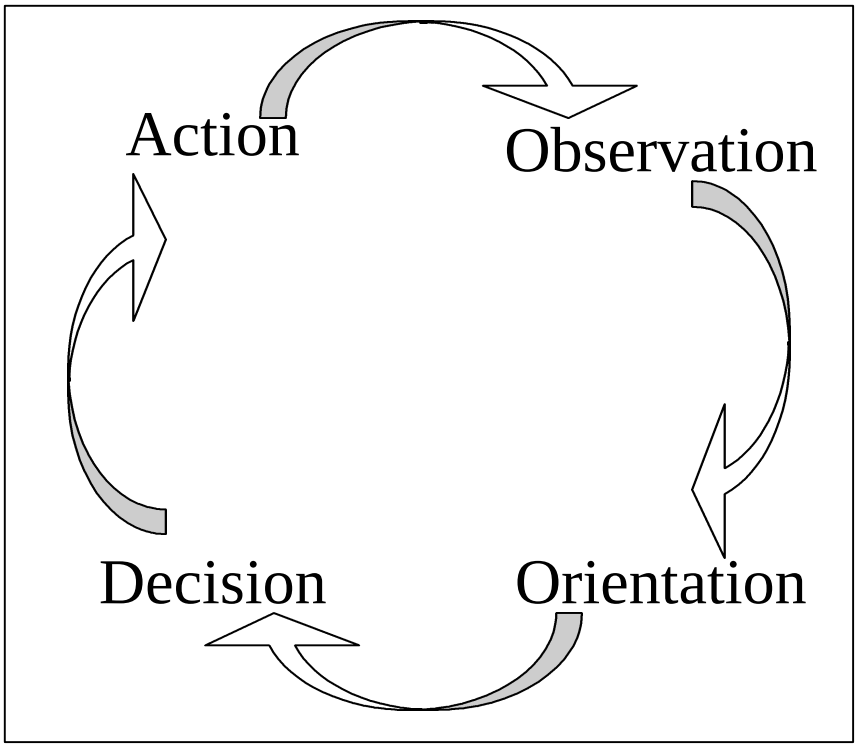


Figure 1. OODA Model taken from
http://www.fas.org/irp/agency/aia/afiwc/index.html, 2000

environments and is consistent with the Naturalistic Decision Making (NDM) paradigm. His model depicts four iterative stages that military commanders go through when making decisions.

The first stage of the OODA Loop is the *observation* stage. In this stage, commanders use their senses to gather situational information. This information may come from first-hand visual observations of actual events or objects, direct or synthesized auditory inputs, and visual representations of actual events or objects via some media.

The next stage is the *orientation* stage. It is in this stage that commanders orient, or make sense from, the information they observed. The Recognition-Primed Decision (RPD) Model proposed by NDM researchers supports this concept (Klein, 1988). The RPD model "emphasizes the importance of situation assessment in expert decision making (Drillings and Serfaty, 1997). The *orientation* stage is, in effect, the military commander's situational assessment of the observed information influenced by his or her previous experience or pattern recognition.

Following the *orientation* stage, the OODA Loop model proposes that military commanders enter the *decision* stage. This stage results in a choice of alternative courses of action. The RPD model postulates that fewer alternatives are generated by experienced decision-makers because they tend to stop generating decisions when the first satisfactory choice is determined (Drillings and Serfaty, 1997). This may explain why military commanders in stressful, fast-paced, ill-defined situations are able to make decisions faster than might be expected by the Rational Decision Making model. Boyd's (1987) *decision* stage is supported by Simon's (1959) satisficing process that occurs in a bounded rationality context.

The final stage, the *action* stage, is when the military commander initiates some action or behavior based on the option decided upon in the *decision* stage. This action may be some behavior, like pulling the trigger to giving an order to launch a missile. It may also result in no observable behavior, for instance the choice not to act.

While the OODA Loop is not rich in empirical support, support for this cognitive process is found in the Rational Choice Model, NDM and other literature (Simon, 1957; Roman, 1999; Kaempf, Klein, Thordsen, and Wolf, 1996; Entin and Serfaty, 1997; Drillings and Serfaty, 1997; Seong, Llina, Drury, and Bisantz, 2000). Therefore, the OODA Loop model provides a useful starting point from which to examine decision-making and how it relates to the human-information system trust relationship in a command and control environment .

Command and Control

The widespread integration of information systems into the modern military command and control (C2) environment provides a unique environment within which people make decisions based, in part, on information received from information systems. Therefore, a review of C2 related literature was performed in order to identify some of the unique elements of military C2 environments that may influence the human-information system trust relationship.

As Roman (1999) and others point out, finding an agreed upon definition of command and control is difficult given the varied and conflicting definitions in the literature (Drillings and Serfaty, 1997). C2 is defined in this study in the same way that Drillings and Serfaty eloquently put it; “Command and control (C2) is the term that

describes the job of the battle commander. C2 is characterized by ill-structured problems, changing conditions, high stakes, and time demands" (Drillings and Serfaty, 1997: 71). Given these uncertainties, risks, and time demands, battle commanders have become reliant upon information systems as tools to help reduce the uncertainty, risk, and time demands. The usefulness and value of these tools is determined by many factors including among them trust in both the information system and the source of the information (Davis, 1986; Dillon and Morris, 1996).

One recent study proposed a framework from which to study human trust in automated decision-making aids in a C2 environment (Bisantz, Llina, Seong, Finger, and Jian, 2000). Bisantz *et al*'s study suggest that one of the most significant factors that influence decision-making in a C2 environment is the threat of an attack by an adversary against the C2 information systems. This military-unique threat is commonly referred to as Information Warfare.

Information Warfare

Information has long been considered a vital element in warfare. Over 2500 years ago, military strategists like Sun Tzu (6th cent B.C.) wrote about the importance of gathering information, both about oneself and the enemy, before going into battle. In addition, his teachings suggest that the wise commander attempts to wage war using the least possible effort. Traditionally, information gathering and battles required the movement of military troops close to an enemy's geographical location. This was costly for the attacker both in terms of time and effort. Additionally, the geographical distance and barriers the attacking force had to traverse afforded the enemy some means of

protection. However, the protection once afforded to economic, social, and military infrastructures by geographical distances, are now increasingly vulnerable because of the connectivity offered by the Internet and due to the reliance upon information systems that control these infrastructures (Van Cleave, 1997). An enemy can now easily, quickly, and covertly attack critical information systems using a wide variety of techniques. Therefore, understanding which of these techniques may effect a military commander's trust in the C2 information systems they rely upon is of great importance to this research.

This study defines information warfare as both the offensive and defensive use of information as a weapon through the exploitation of information technologies. Arguably, there are a multitude of perspectives and definitions of information warfare (Van Cleave, 1997; Kuehl, 2000; Cornerstones of Information Warfare, 1996; Whitehead, 1999). While there may not be agreement on a common definition, there are commonalties among the information warfare tactics and weapons suggested in these writings, such as software viruses, denial of service attacks, and information manipulation.

The versatile and ubiquitous nature of the Internet has spawned the creation of a variety of information warfare weapons and tactics (Van Cleave, 1997). Direct launch is a tactic that describes the indiscriminate employment of software viruses and logic bombs. These software viruses and logic bombs cause software application, operating systems, and sometimes hardware damage to any system that becomes infected. Forward basing is similar to "direct launch", except that these software viruses lie dormant until a specific action triggers its activation. Hacking is another tactic where unauthorized persons gain access to information systems. Hackers gain access for a variety of motives including curiosity, theft of information, or the intentional manipulation of information.

Information Manipulation Theory

The intentional manipulation of information poses, perhaps, the greatest threat to modern military command and control centers (Kuel, 2000; Everett, DeWindt, and McDade, 2000). The potential damage that can be caused to an adversary by creating false information in their command and control systems is potentially enormous. A recent Air Force News article painted a vivid picture of this type of attack:

> Imagine if you told an F-16 Fighting Falcon pilot to attack a target 550 miles away, and then learned the plane's maximum range was only 500 miles. Or suppose you ordered a C-5 to deliver cargo to an airport where the runway was too short for the plane to land. (Mayer, 21 Jun 2000)

This example illustrates the chaos made possible by the intentional manipulation of information in a C2 system. The model of intentionally manipulating data is not new or unique to the information age. A recent Information Manipulation theory was proposed to describe deception in communication (McCornack, Levine, Morrison, and Lapinski, 1996). This theory suggests that violation of one or more of the maxims (quantity, quality, relation, and manner) results in a deceptive communication. While not rich, some support for this theory is found in the literature (Yeung, Levine, and Nishiyama; 1999, Biros, 1998). For instance, the intentional manipulation of the number of enemy troops in a C2 information system violates the maxim of quality and, therefore would be classified as information manipulation. The information manipulation theory also suggests that the intentional manipulation of information may influence a decision maker to make a decision that is different from what they would have made given the original information. Since this theory suggests that information manipulation can

influence a decision-maker, and because decision-making in a C2 environment using information systems suggests trust between the military commander and C2 information systems, it is important to understand what trust is and what other factors may influence trusting behavior.

Theories of Trust

A common thread throughout each of the previous sections is trust. Therefore, before a framework can be developed to study the overall research question, a thorough review of trust research is necessary.

Theories and philosophies on trust can be found throughout history. The ancient Greek philosopher, Aristotle, began his great work, Metaphysics, by asserting that man should trust the sense of sight above all others (Kirwan, 1993). Aristotle does not clearly define trust, however the definition suggests a *belief* in something. Vague definitions of trust, like Aristotle's are not the exception. Throughout recorded history, the term "trust" has been either vaguely or narrowly. This causes difficulties for scholars who wish to study and compare trust research (Golembiewski and McConkie, 1975). In the last century, trust has been defined across the spectrum of academic disciplines. In one study, a review of trust literature found divergent definitions of trust across the disciplines of management, communications, sociology, economics, political science, psychology, and social psychology (McKnight and Chervany, 1999). As McKnight and Chervany (1999) point out, trust is too broad a concept to define narrowly. Therefore, a literature review of trust research is presented below. The purpose of the review was to find a suitable model of trust broad enough in scope to allow cross-disciplinary studies and robust

enough to examine the trust relationship between people and information systems, especially in C2 environment.

Human Trust in Information Systems

The vast majority of trust research found deals primarily with trust between and among humans. However, with the advent of the computer age and with the increasing role information systems play in society, there are a growing number of studies on the trust relationship between humans and information systems. Examples of how important and integral information systems have become in American society are plentiful. Information systems are used for everything from exchanging information between businesses, assisting pilots to operate aircraft, controlling nuclear power plants, and directing military forces in battle. The critical nature of these tasks underscores the need to understand the human-information system trust relationship.

One such study (Zuboff, 1988) looked at how people trust automation in the workplace. This research found that workers tended to either distrust the technology resulting in the lessened use of the automation or over trust in the automation resulting in problems when the automation subsequently failed (Zuboff, 1988). Zuboff's observations have been widely supported in empirical studies (Muir, 1987; Muir and Moray, 1996; Mosier, Skitka, and Burdick, 2000; Seong, Llina, Drury, and Bisantz, 2000).

Some of the most cited of these empirical studies are Muir's trust in automation experiments (Muir, 1987; Muir, 1994; Muir and Moray, 1996). Muir's experiments consisted of having subjects perform a task on system simulators that had both manual

and automated controls. The subjects either experienced random errors with the automated control, consistent errors, or no errors. Muir measured the subjects trust in the system throughout the duration of the experiment.

Muir's findings were consistent with that of Zuboff and others (Sheridan and Hennessy, 1984; Wiener and Curry, 1980). She found that workers monitoring automation became complacent when the automation was perceived to perform correctly. Similarly, she found workers spent more time monitoring systems considered to be error prone (Muir, 1994). In addition to these findings, Muir found evidence to suggest that following a perceived error, a person's trust will degrade but will gradually recover over time. Her findings have been supported in similar studies (Lee and Moray, 1992; Bisantz, Llina, Seong, Finger, and Jian, 2000).

To measure trust in automation, Muir incorporated Barber's (1983) taxonomy of trust and Rempel, Holmes, and Zanna's (1985) taxonomy of the development of trust as a basis for a model specifically tailored towards human trust in automation. Her model of trust consists of three dimensions of expectations: Persistence, Technical Competence, and Fiduciary Responsibility. Each of these dimensions are crossed with three levels of experience: Predictability, Dependability, and Faith (see Figure 2 next page).

Persistence is defined as "an expectation of constancy" (Muir, 1994, 1910). This suggests a fundamental assumption or expectation by people that physical and social laws exist and are predictable and stable in nature. For instance, man is good, gravity will continue to make things fall, and electrons will continue to spin about the nucleus of atoms (Barber, 1983). The definition of technical competence is more specifically

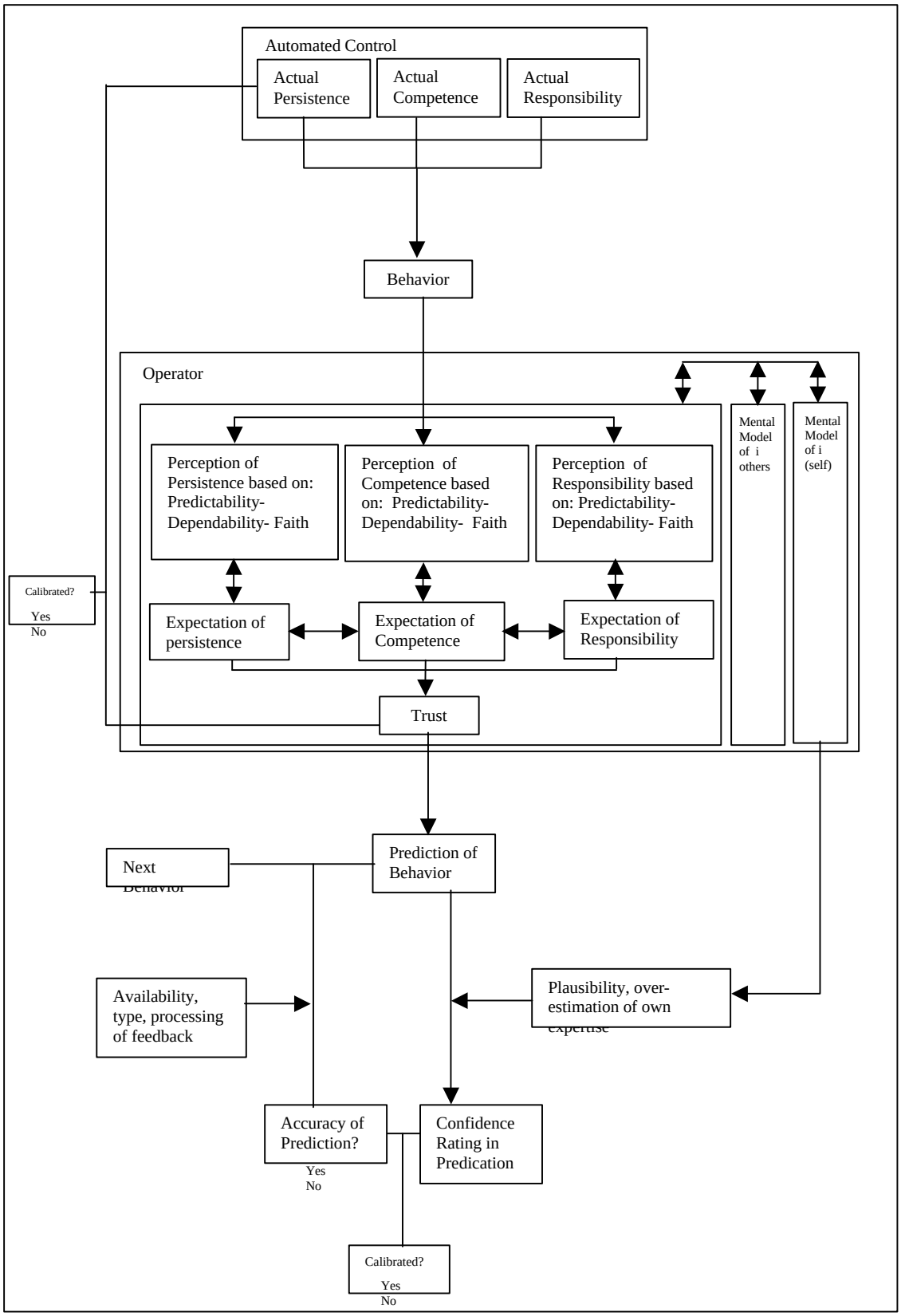


Figure 2. Man-Machine Model of Trust taken from Muir (1994)

tailored towards automation than is Barber's (1983) definition of competence. Here, Muir defines technical competence as it pertains to some automated system. This technical competence consists of "expert knowledge, technical facility, or routine performance" (Muir, 1994: 1910-1911). This concept suggests humans come to expect machines to perform a given or programmed task correctly. The final dimension in Muir's model is that of fiduciary responsibility. This is defined in situations where "a trustor's own technical competence is exceeded by the referent's, or when the competence of another is completely unknown" (Muir, 1994: 1911). In terms of a person's trust in an information system, an example of this would be a person's trust in the benevolence or intentions of the system designer (Barber, 1983; Muir, 1994).

Muir and others believe that trust is "a hierarchical stage model, where trust develops over time, first depending upon predictability, then dependability, and finally faith" (Lee and Moray, 1992: 1245). This model of trust is consistent with the cyclical nature of decision-making as offered in the OODA Loop model (Boyd, 1987). However, other trust research suggests some facets of trust not encorporated in this model. Therefore, the search for a model that encompasses these additional facets, especially those useful to examine trust in a military environment was continued.

Automation Bias

Muir measured the constructs of fiduciary responsibility, technical competence, and trust behavior using survey instruments and observed behavior. Human factors researchers often use observed behavior as a measure of trust, especially in the widely studied population of aircrews. (Mosier, Skitka, and Heers, 2000; Mosier, Skitka, and

Burdick, 2000). In these studies, subjects participated in controlled experiments using the aid of an auto pilot system to control a simulated aircraft. The goal of their research was to study the suggestion that air crews "…have a tendency to over-rely on automation to perform tasks and make decisions for them rather than using the aids as one component of thorough monitoring and decision-making processes" (Mosier, Skitka, and Heers, 2000: n. pag.). This phenomenon, which they call "automation bias" is consistent with Zuboff's (1988) study. This study found a significant number of experienced airline pilots caused both automation omission errors (i.e. failing to take appropriate action because the auto pilot system did not provide information) and automation commission errors (i.e. committing an error based on erroneous information presented by the auto pilot system). This study, and others found significant evidence that this cognitive bias (i.e. automation bias) exists and may be due to excessive reliance on these trusted systems (Mosier, Skitka, and Heers, 2000; Mosier, Skitka, and Burdick, 2000).

Truth Bias

The phenomenon of automation bias is consistent and similar to another theory called "truth bias" offered by McCornack *et al* (1996). Truth bias suggests that as people develop trusted relationships with others, they tend to believe what is told to them by the trusted person without verifying the information. The truth bias theory was later extended to include a person's trust in information system artifacts (Biros, 1998). Biros examined the effects of intentional manipulation of information within the framework of his proposed "artifact truth bias" model. Automation bias, truth bias, and artifact truth bias are all consistent with the findings of Zuboff (1988) and offer support to the notion

that people trust information systems in the same way they trust other people. Furthermore, automation bias and truth bias suggests that decision-makers who rely on and trust information systems may be susceptible to information warfare tactics like information manipulation.

Applicability to Trust in Information Systems

The studies of trust in automation presented above offer strong evidence that a person's trust or trusting behavior in information systems is possible to model, measure, and predict. However, the models of trust used in these studies are somewhat limited in scope. Muir's model of trust, for instance, fails to measure the full dimensions of trust. While her model (see Figure 3) accounts for a mental model of others (i.e. a disposition to trust), it fails to further break down, define, and measure the various types of this dispositional trust. For example, a person's disposition to trust may be situational in nature or a general assumption based on previous beliefs (McKnight and Chervany, 1999; Riker, 1971; Kee and Knox, 1970). Likewise, while the studies of automation and truth bias observed behavior as a means to measure trust, they failed to adequately define and measure specific factors of trust. Examples of these specific factors include the situational nature of trust and a more general disposition to trust. Additionally, none of these studies defined or measured the influence that trust in external safeguards, either organizational or technical, have on a person's trusting behavior. Despite this, the framework used in these studies are useful in developing a new framework within which the trust relationship between people and information systems can be more fully examined.

Theory of Reasoned Action

Most of the trust research described in the previous sections have looked at trust as a behavior (Muir, 1994; Muir and Moray, 1996; McCornack et al, 1996; Mosier, Skitka, and Heers, 2000; Mosier, Skitka, and Burdick, 2000). Therefore, a search for a model that predicts trust as a behavior was performed. This search found that most such models designed to predict behavior are grounded in Fishbein and Ajzen's Theory of Reasoned Action (TRA) (1975). The TRA model has been widely cited and used as the basis for several predictive behavioral models. For instance, Davis' Technology Acceptance Model (TAM) (1986) has been used successfully to predict the attitudes and behavior of people towards technology. This provides evidence that the TRA model may be useful in predicting trusting behavior towards technology.

The TRA (see Figure 3 next page) suggests a person's behavior can be predicted by first understanding the person's intention to carry out the behavior, which in turn is determined by both the person's attitude and subjective norm (Fishbein and Ajzen, 1975). Each of these two constructs, attitude and subjective norms, are influenced by some preexisting belief structure.

In the case of attitude, Fishbein and Ajzen (1975) suggest that a person's attitude can be influenced through a change in the person's belief about the consequences of their actions. Their belief in the consequences of their actions can be influenced by some external stimulus (Fishbein and Ajzen, 1975, Dillon and Morris, 1996). Likewise, the person's normative beliefs and motivation to act can influence the construct of subjective norms. This belief and motivation is also influenced by some external stimulus (Fishbein and Ajzen, 1975).

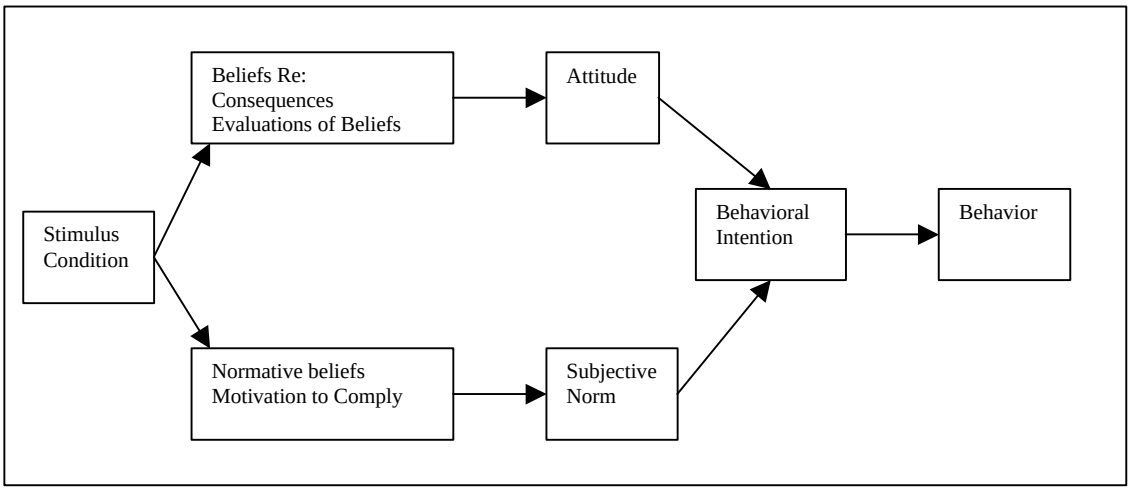


Figure 3. Theory of Reasoned Action model taken from Dillon and Morris (1996)

McKnight and Chervany's Model of Trust

McKnight and Chervany's (1999) theoretical model of trust is based on TRA and is broad enough in scope and robust enough to use in this research. This model's breadth of scope is rooted in Tiryakian's (1968) attempt to organize and fully categorize the various definitions of trust. Tiryakian's categorization effort was extended by McKnight and Chervany (1999) who created two conceptual typologies of trust: "typology type (a)—a classification system for types of kinds of trust; typology type (b)—a set of six related types of trust constructs resulting from the analysis of the classification system (Tiryakian, 1968)" (McKnight and Chervany, 1999, 3). From these classifications and typologies, McKnight and Chervany developed a model of trust that incorporates the broad scope of these various components (see Figure 4 below).

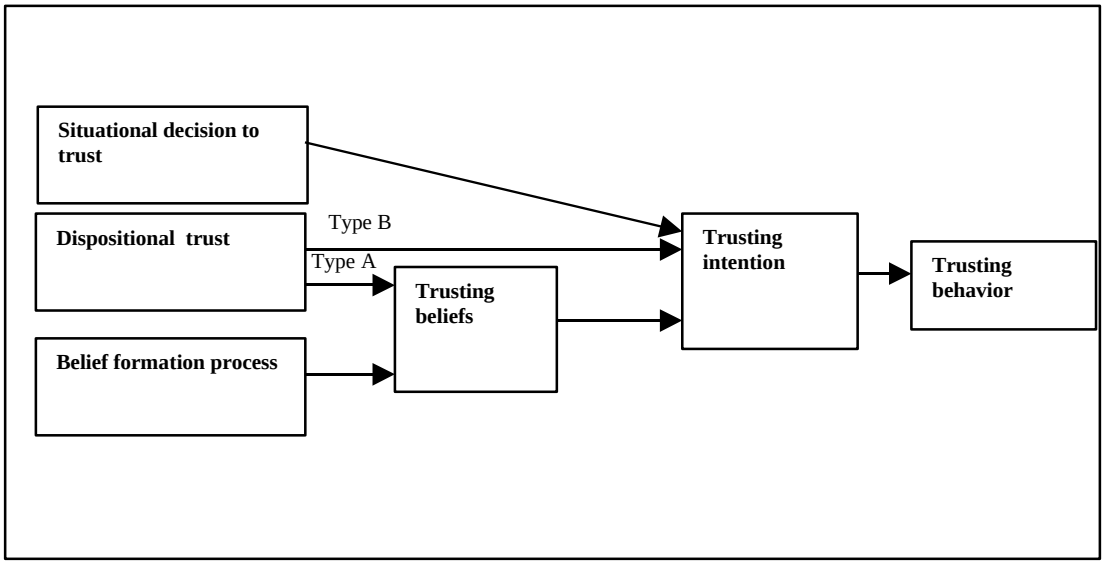


Figure 4. McKnight's Model of Trust drawn from
(McKnight and Chervaney, 1999)

Trusting behavior is treated in this model as a latent construct capable of being measured by indicators (McKnight and Chervany, 1999, Riker, 1971). For instance, taking a prescribed medication based on the recommendation of a doctor is not, in itself trust, but rather an indicator of trust. These indicators take many forms, but in essence each indicator can be defined as "…any act of dependence or increasing dependence" on another person or object (McKnight and Chervany, 1999, 26). The concept of reliance and dependence are often found in trust literature (Barber, 1983; Mayer, Davis and Schoorman, 1995; Muir, 1994; Sheridan and Hennessy, 1984). One type of trust indicator is the act of making a decision based on the actions of another despite a possible loss or negative consequence (Anderson and Narus, 1990).

The trusting behavior construct is supported by a person's intention to trust. McKnight and Chervany define trusting intention as "the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security,

even though negative consequences are possible" (McKnight and Chervany, 1999, 23). The five essential components of this construct include a possible negative consequence, a dependence on the person or object, a relative feeling of security, a lack of or willingness to relinquish control, and all within a given situational context. (Bonoma, 1976; Giffin, 1967; Dobing, 1993; Rempel, Holmes, and Zanna, 1985; Gabarro, 1978; Lawler and Rhode, 1976; Anthony, 1965). This construct is difficult to observe and is often measured through some instrument, such as a survey or questionnaire.

In the same way trusting intention supports trusting behavior, a person's "cognitive beliefs and belief-related confidence" support the trusting belief (McKnight and Chervany, 1999, 26). McKnight and Chervany (1999) conclude that trusting belief consists of four main elements: benevolence, honesty, competence, and predictability (Bromiley and Cummings, 1995; Dobing, 1993; Gabarro, 1978). Benevolence is the extent one is concerned with the welfare of another. Honesty is defined in terms of truthfulness and making good on an agreement. Competence is defined as having the ability to do what needs to be done. Finally, predictability is defined as actions that are consistent enough to enable a forecast of a future action in a given situation.

As mentioned before, trust is situational in nature (Riker, 1971; Kee and Knox, 1970), therefore the construct of situational decision to trust is defined as "the extent to which one intends to depend on a non-specific other party in a given situation" (McKnight and Chervany, 1999, 29). This construct directly supports trusting intention, rather than trusting belief, because it is not related to a specific person or object, but rather to a specific situation.

Unlike situational decision to trust, McKnight and Chervany (1999) propose a construct that is situationally independent, disposition to trust (Harnett and Cummings, 1980; Wrightsman, 1991; Rotter, 1967). Disposition to trust is the extent to which a person "has a consistent tendency to trust across a broad spectrum of situations and persons" (McKnight and Chervany, 1999, 29). They suggest there are two types of dispositional trust: Type A and Type B. Type A dispositional trust is a kind of general assumption by a person that other people or objects are trustworthy. Type B dispositional trust, on the other hand, does not make any such assumption. The disposition to trust is based on the belief that the result of the trust will be better than if they did not trust (McKnight and Chervany, 1999). Because Type A is specifically related to the person or object of trust, it supports trusting belief. However, Type B is related to the outcome, therefore Type B supports trusting intention (McKnight and Chervany, 1999).

The final construct in this model of trust is system trust. System trust is defined as the "extent to which one believes that proper impersonal structures are in place to enable one to anticipate a successful future endeavor" (McKnight and Chervany, 1999, 28). In this case, a person's trust in another person or object is not based on any belief or attitude towards that person or object, but rather based on the attitude or belief in a safeguard of some external entity (Shapiro, 1987, Luhmann, 1991; Zucker, 1986). System trust directly supports trusting intention because it "act[s] like a safety net" and reduces the level of risk and uncertainty (McKnight and Chervany, 1999, 28).

Applicability to Human-Information System trust

McKnight and Chervany's model of trust meets the criteria set forth in this study to capture the breadth and scope of the trust concept. This model encompasses the trust theories of leading researchers across academic disciplines, including Muir's research on trust in automation, and provides a means for a comparative analysis between this study and previous research in automation trust. While not all of the constructs in McKnight and Chervany's model will be studied, some of their constructs lend themselves nicely to examining the unique nature of C2 operations. Therefore, this model will be used as a framework to study human trust in information systems within a command and control environment where an Information Warfare threat exists. This modified model, along with research hypotheses, are presented in the next section.

Research Hypotheses

The hypotheses proposed in this section are largely based on relationships between the various constructs found in McKnight and Chervany's model of trust, simplified

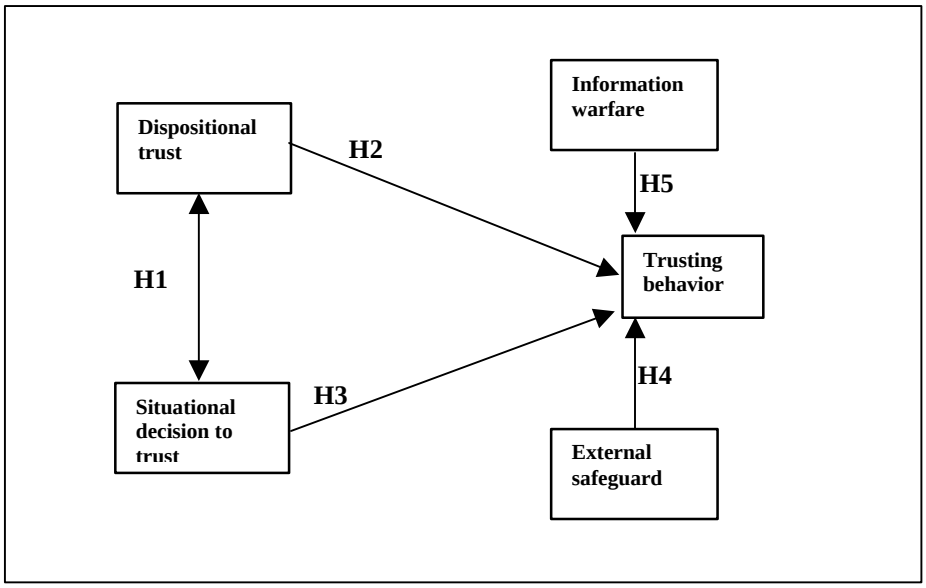


Figure 5. Adapted Model of Trust drawn from
(McKnight and Chervaney, 1999)

below in Figure 5 on previous page. As mentioned in the previous section, not all of the constructs in McKnight and Chervany's model were used in this study. Of these constructs, dispositional trust and situational decision to trust are likely to be useful in examining the research question. As evidenced in the automation bias and truth bias studies (Mosier *et al*, 2000; Bios, 1998), people will demonstrate a trusting behavior (e.g. shutting down an engine given a fire indication light) if they have a preconceived trust for that type automation (fire indication light). The construct of dispositional trust captures this facet of trust. However, it would be useful to determine trusting computers in general is more useful to predicting trusting behavior than trusting computers in specific situations. The latter is captured in the construct of situational decision to trust. This proposed model (see Figure 6 previous page) also includes a construct called external safeguards, which is captured in McKnight and Chervany's construct called system trust. Finally, a construct of information warfare was included in order to study the effect of this military-unique factor on trusting behavior in a C2 environment. The complete definitions for each of the constructs in the proposed model can be found in Table 2 on the next page.

Table 2: Definition of Constructs taken from McKnight and Chervany (1999)

Construct 1. Situational decision to trust
Definition: The extent to which one intends to depend a person or object in a given situation.

Construct 2. Dispositional trust (Faith in Technology's Competence)
Definition: The general tendency of one to believe in the reliability of a person or object in a given situation.

Construct 3. External safeguard

Definition: The extent to which one believes (consciously or unconsciously) that an impersonal safeguard exists, such that it supports their trust a person or object.

Construct 4. Information warfare

Definition: One's perception of erroneous or altered information caused by an adversary whose intent is to mislead or cause a person to behave in a way contrary to how they would have otherwise behaved.

Construct 5. Trusting behavior
Definition: An action or inaction that indicates the intent to trust a person or object despite the possibility of negative consequences.

Hypotheses Development

McKnight and Chevany's model of trust includes two types of dispositional trust: Type A and Type B. As defined earlier in this chapter, type A dispositional trust is a kind of general assumption that people or objects are trustworthy and, therefore will have a

direct influence on a person's intention to trust and consequently their trusting behavior (McKnight and Chervany, 1999).

Another type of trust offered by McKnight and Chervany (1999) is situational decision to trust. Situational decision to trust means that trust has been formed from a person's past experience based on a particular situation rather than a belief about a specific person or object (Riker, 1971).

While McKnight and Chervany (1999) show disposition to trust and situational decision to trust as two independent constructs, it is likely that a person's disposition to trust (type A) will have some affect on their decision to trust information systems in a given situation. The reverse of this relationship may also be true. In other words, a persons decision to trust a person or object in a given situation may influence their general beliefs or attitudes about that person or object. This relationship seems likely since both attitudes are formed from some previous experience, and perhaps the same experiences (Erikson, 1968; Roter, 1967; McKnight and Chervany, 1999). This study proposes that it is likely that disposition to trust and situational decision to trust will be positively correlated to each other.

H1: Disposition to trust Information Systems and situational decision to trust are positively correlated with each other.

The TRA model suggests a person's behavior can be predicted by first understanding the person's intention to carry out the behavior, which is determined by both the person's attitude and subjective norm (Fishbein and Ajzen, 1975). However, sometimes it is difficult or impossible to measure a person's intention to do something

(Morris and Verkatesh, 2000). This is the case in the dynamic and fluid environment of military command and control that is being studied here. Additionally, intention to trust is often used as a surrogate for behavior when behavior can not be measured (Morris and Verkatesh, 2000). Therefore, intention to trust is eliminated from this model and all relationships between other constructs and intention to trust will be shown to lead directly to trusting behavior.

As defined earlier, dispositional trust influences a person's trusting behavior. This type of disposition to trust is often found in military battle commander's who form a general trust for the people and equipment that they work with (Ericson, 1968; Boyd, 1987). An example of this is a general trust in information systems to provide the necessary information for a battle commander to make a decision. This study suggests that dispositional trust will have a positive influence on a person's trusting behavior.

H2: Disposition to trust Information Systems positively influences trusting behavior.

The studies in NDM show evidence that decision-making is situational in nature. The Recognition-Primed Decision (RPD) Model describes the importance of the situation with respect to forming a decision ((Klein, 1988, Drillings and Serfaty, 1997). Boyd's (1987) decision-making model supports this theory by suggesting that during the orientation stage, the military commander's assessment of the observed information is situational in nature. Following the orientation stage, Boyd (1987) suggests military commander's make a decision.

The literature also suggests that the more positive experiences a decision-maker has with objects, like information systems in given situations, the more likely they will trust the object (Mosier, Skitka, and Heers, 2000). This phenomenon was observed in studies that examined automation bias in airline pilots. Experienced airline pilots tended to take action (i.e. trusting behavior) based solely on the information received from an automated decision support system in certain situations (Mosier, Skitka, and Burdick, 2000). Given the findings by Mosier *et al* (2000) that a positive attitude or belief in a system will lead to a behavior, this study proposes that McKnight and Chervany's (1999) attitudinal construct of situational decision to trust will positively affect trusting behavior.

H3: Situational decision to trust Information Systems positively effects trusting behavior.

The United States military is functionally organized. Each unit has a specific set of mission objectives. Often, a unit's mission objective may be to safeguard some other unit. Military personnel are conditioned to trust these units do their job so that they may in turn accomplish their own mission objectives. Weick and Roberts (1993) observed this behavior on the flight deck of a navy aircraft carrier and termed this behavior "collective mind." The literature supports this organizational form and mode of operation in that it suggests a person's decision to trust is influenced by the belief that some external organization or entity exists to provide a safeguard to the decision maker (Luhmann, 1991; McKnight and Chervany, 1999) However, the literature is not rich in empirical studies of this facet of trust. In fact, most of the trust research that explores the human-automation trust relationship examines situations where either the automation

malfunctions and no external safeguard exists. This study proposes that the construct of external safeguards will have a positive effect on a decision-maker's trusting behavior.

H4: External Safeguards will have a positive effect on trusting behavior.

Much has been theorized about the effects of information warfare on decision-makers, but little empirical research exists (Van Cleave, 1997; Kuehl, 2000; Whitehead, 1999). What little empirical evidence does exist, suggests that the perception of information warfare events, such as computer viruses or information manipulation, will have a negative effect on decision-makers (McCornack *et al*, 1996; Biros, 1998; Yeung, Levine, and Nishiyama, 1999; Seong, Llina, Drury, and Bisantz, 2000). Therefore, this study proposes that the perception of an information warfare attack, such as information manipulation, will have a negative effect on trusting behavior.

H5: The presence of information manipulation will have a negative effect on trusting behavior.

Summary

In summary, the goal of this research was to examine the influence that External Safeguards (i.e. System trust) and Information Warfare (i.e. Information Manipulation) has on decision-making in a naturalistic decision making environment, as well as attitudes such as dispositional trust and situational decision to trust. To examine these effects, an experimental design will be presented in the next chapter that incorporates the theoretical framework established in this chapter. McKnight's model of Trust (McKnight and Chervany, 1999), decision making theories (Orasanu and Connolly, 1993; Boyd,

1987; Roman, 1999), and information warfare theories (Whitehead, 1997; McCornack, 1996; Biros, 1998) were used to build this framework from which trusting behavior can be observed and measured. A series of hypotheses were proposed based on supporting research, as well as gaps and weaknesses in existing research.

The following chapter will operationalize the constructs defined in this chapter and offer a methodology to capture data that can be used to test the hypotheses presented in this chapter. Finally, the methodology will incorporate the characteristics necessary to create a naturalistic military decision-making environment.

III. METHODOLOGY

(Experiment 1)

Overview

The first chapter of this thesis described the research problem of interest to this study. The second chapter laid a theoretical foundation by presenting a review of trust, decision-making, and IW literature and then built a theoretical framework from which the research problem could be explored. Finally, a set of hypotheses was offered to predict the type of relationships between the constructs of interest. This chapter describes the methodology used in the first experiment to test the hypotheses, operationalizes each construct of interest by applying the theoretical framework established in Chapter II, and defines a set of variables that were used to measure each construct. Finally, the data collection process is described, along with the statistical methods used to analyze and make inference about the data. The methodology for the second experiment is described in Chapter V.

Experimental Design

In order to investigate a person's trusting behavior in an IW domain, a military command and control (C2) scenario was developed for use with a high-fidelity computer simulator, the Distributed Dynamic Decision-making (DDD) simulator developed by Aptima, Inc. This high-fidelity system produced a *microworld* within which subjects were immersed into a complex C2 computer simulation (Brehmer and Dorner, 1993). Computer simulated microworlds offer a bridge between laboratory and field experiments

by providing a realistic and naturalistic environment and greater experimental control. While this experiment was conducted in laboratory setting, the high-fidelity DDD system closely simulates a real-world C2 decision-making environment (Entin, Kerrigan, Serfaty, & Young, 1998). The DDD system allowed for the collection of quantitative measures over the course of each experimental trial, as well as measurable attitudes and beliefs through a pre and post survey questionnaire.

The experiment was designed as a between group experiment which manipulated two independent variables from the theoretical model described in the last chapter, External Safeguard and Information Warfare. These variables were completely crossed to a 2 X 2-design configuration as seen in Figure 6 below. Each subject experienced only one of the four possible conditions.

		External Safeguards	
		High	Low
Information Warfare	No Attack	**Treatment Gp 1**	**Treatment Gp 2**
	Attack	**Treatment Gp 4**	**Treatment Gp 3**

Figure 6. Group Configurations

Each subject was given training on the weapon system concept and computer interface. A further description of the training is described in the Tasks and Procedures section of this chapter. Following training, each subject was tasked by the experiment administrator (acting as an Air Force Research Laboratory field evaluator and reading from a script) to perform a hidden-profile, decision-making task that involved the control of multiple Unmanned Combat Aerial Vehicles (UCAV's) to defend one of four air space zones on the computer display (see Appendix 1). Control of each UCAV was performed through various user actions on the DDD system. The UCAV system was described to the subjects as a new operational C2 system being field tested by Air Force Research Laboratories.

Subjects were tasked to identify incoming air tracks by electronically directing UCAVs to move within sensor range. Air tracks are a computer representation of an aircraft radar signature displayed on the subject's computer display. If the air track was identified as a hostile, they were authorized to attack the target without the need for further verification.

They were told the objective of their mission was to stop all hostile tracks before they entered protected airspace (see Appendix 2). Subjects were told that the UCAV computer system could automatically determine the identity of any air track once it was within the UCAV's sensor range. They were also told the computer system was 100 percent accurate in both algorithmic and display processing.

Subjects were cautioned that information from the UCAV aircraft and the computer system traveled across an unclassified local area network (LAN) and was

therefore vulnerable to Information Warfare attacks. They were further cautioned that the simulation might contain a simulated IW attack against the LAN. Subjects were given a means to communicate electronically with an orbiting Air Warning and Control System (AWACS) aircraft to verify the identity of air tracks, once the air tracks had been identified by their UCAV.

Five minutes into the simulation all subjects received a threat message from a simulated network participant; the Network Security Force (NSF) that indicated an attempted attack against the network had occurred (see Appendix 3). During training, subjects were told the role of the NSF was to monitor and protect the networks in the region against IW attacks. Two new tracks appeared approximately 10 seconds following the message from the NSF. For treatment groups three and four, one of these tracks appeared as a friendly when in fact it was a hostile. The other track appeared as a hostile when it was actually a friendly. If the subjects destroyed the friendly aircraft, a visual and audible alarm was triggered indicating a fratricide had occurred. In addition, subjects could perceive this error by observing a decrement to their defensive score.

Indication of the other spoofed track (i.e. hostile track that was spoofed as a friendly) included a visual que of a steady decrement to the subject's defensive score if the air track entered the subject's protected air space. Additionally, subjects were able to perceive the destruction of their assets (i.e. tanker aircraft and bases) once the hostile aircraft flew within weapons range of the subjects assets.

To give the experimental task a sense of realism and urgency, a scenario briefing was provided to each subject to read before the start of the experimental trial (see Appendix 4). The scenario briefing laid out a realistic military threat environment in

which an attack of enemy aircraft loaded with weapons of mass destruction was imminent. In addition to the scenario, the experiment facilitator explained the scoring system (see Appendix 5) used during the simulation. The scoring system was designed to simulate the high-risk environment of combat C2 operations. Subjects were told that their overall score would be used to determine the success of the mission.

Pilot Study

A pilot study using Air Force Company Grade Officers (Ss =10) was performed to ensure the experiment was feasible, safe, and met the stated objectives. Air Force Company Grade Officers are a superset of the population studied (i.e. Air Battle Manager Officers). This test helped identify potential problems with subject reactivity and game play. For instance, a manageable number of incoming tracks was determined. It was important to find a number of tracks that kept the subjects engaged in the game, without falling into one of the common errors of computer-simulated microworlds, *task saturation* (Brehmer and Dorner, 1993). Brehmer and Dorner (1993) define task saturation as overwhelming the subjects with too many assigned tasks to perform. This type of error could result in measurements of something other than the intended measure or a reduction in the strength of experimental manipulations.

Another finding from the pilot study was that the construct of Trusting Belief proved difficult to measure. During the pilot study, subjects complained that they were unable to answer questions that measured Trusting Belief in the UCAV system because they had no previous experience or frame of reference for this system. Therefore, a uniform level of trust in the UCAV operation system was controlled for during the

training session. This was accomplished by teaching the subjects about the individual components of the UCAV system during training and emphasizing that the UCAV system was 100 percent accurate in processing and displaying sensor information. Next, the unmanned sensor aircraft were described. Subjects were again told that testing proved the unmanned sensor aircraft to be 100 percent accurate. This control was checked by the subject's response to a question on the pre-trial multiple-choice test (see Appendix 5).

Subjects

A random sample (Ss=56) of AWACS operators were recruited from the 552nd AWACS Operations Group at Tinker Air Force Base, Oklahoma to participate in this study. The ages of subjects ranged from 19 to 46 years old and their experience ranged from 0 to 50 hours of combat C2 experience. Their military ranks ranged from junior enlisted to field grade officer.

Equipment and Facilities

All experiment sessions were run in an office with no windows and a single entrance (see Appendix 7). Each subject performed his or her tasks in a workspace that was isolated with a partition system. While each subject could not visually see another subject's computer display, the partitions were not sufficient to prevent subjects from hearing each other's comments. Therefore, each subject was told that a communications blackout was in effect and any verbal communication would alert the enemy to their location. Each subject's workspace consisted of a chair, a desk surface, a PC-type laptop

computer system loaded with a Linux operating system and DDD software, and quick reference sheets that defined icons and scoring information.

The room was also equipped with a VHS video player and 25” television set. In addition, a desktop PC-type computer was setup to run Microsoft’s PowerPoint application. These items were used during the training portion of the experimental trial.

Tasks and Procedures

Three experimental trials were scheduled each day, with the exception of the last day, which only had two trials. Each trial lasted approximately two hours (see Figure 8). The experiment ran for five consecutive days, resulting in 14 experimental trials. Treatments were randomly assigned by means of a randomized block design (see Appendix 7).

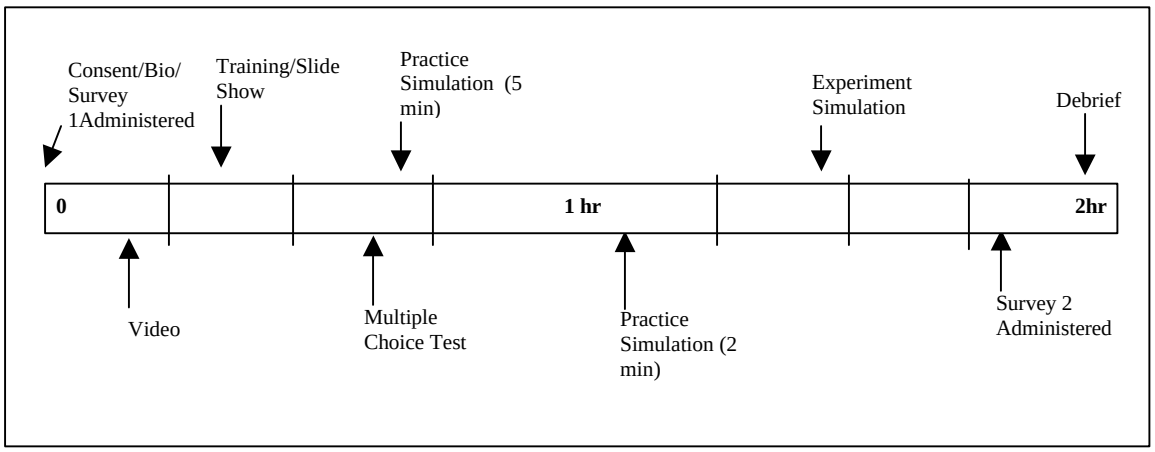


Figure 7 Experimental Time-line

On the scheduled test day, subjects were instructed to report to the evaluation room. Subjects were assigned an operator position (i.e. DM1, DM2, DM3, or DM4)

based on the order in which they arrived (see Appendix 7). Upon arrival, each subject was asked to sign a log-in sheet and was then directed to an operator position. An introductory package was provided to each subject. The package included a standard consent form and a biometric data collection form (see Appendix 9 and 10). Subjects were asked to fill-out each form before the start of the experimental trial.

The experiment facilitator (reading from a script) started the trial by explaining the purpose of the experiment. The facilitator then showed a 3 ½minute training video on the UCAV aircraft and its concept of operations. Following the video, the experiment facilitator went through a PowerPoint training presentation on the desktop PC located in the room (see Appendix 11). Following the video, the subjects were given an opportunity to ask questions. The subjects were then instructed to take their place at their stations. The experiment facilitator instructed each subject to begin the training simulation by clicking the Start button. Subjects were individually shown how to perform the various functions needed to operate the system. The experiment facilitators freely answered questions. This first hands-on session lasted approximately six minutes. Following this session, one of the experiment facilitators briefed the subjects on the training mission scenario, while the other facilitator prepared the computers for the next session. Once the briefing was complete, subjects participated in a 20-minute training simulation session. Again, the experiment facilitators provided assistance to subjects on system operation and game play rules. Following the training session, subjects were given a set of post-training survey forms to complete (see Appendix 12 and 13). They were instructed to put the completed forms in the blue folders provided at each station. They were then given a 5-10 minute break.

Following the break, subjects were asked to resume their positions at their workstations. The experiment facilitator instructed subjects to read the scenario brief (see Appendix 14) and then gave final instructions. Once all subjects indicated they were ready to begin, the subjects were instructed to start the simulation. Subjects were instructed to raise their hands to request assistance if they encountered a computer malfunction or procedural question. Finally, subjects were instructed to remain at their workstation at the completion of the experiment until otherwise directed by the experiment facilitator.

When the simulation ended, one of the experiment facilitators saved the automatically recorded data logs onto floppy disks, while the other passed out post-trial survey forms (see Appendix 15 and 16) and instructed subjects to complete them. Again, each subject was asked to put completed forms into the blue folder at their station and wait until all of the subjects were finished.

Once all subjects finished, the experiment administrator revealed the true purpose of the experiment. An informal question and answer session was conducted at that time. It was interesting to note that even after subjects were told the true purpose of the experiment was not to evaluate the UCAV system, but rather to measure trust in an automated C2 system, subjects continued to provide opinions and suggestions for the UCAV operational system. This indicates that the true purpose of the experiment was not compromised.

Experiment Manipulations

The first experiment manipulation was the construct called external safeguards. External safeguards was operationalized in the form of a simulated game participant called the Network Security Force (NSF). The NSF was described as an external agency that was not actually part of the UCAV system. Subjects were told that the NSF's role was to monitor and protect the LAN against IW attacks. The NSF was, in essence, an external safeguard that contributed to the subject's sense of normality and confidence by providing alerts to the subjects of IW attacks. Treatment groups one and four were told by the experiment facilitator that the NSF was very effective (90%) at detecting enemy information attacks and defending the network against these attacks. Treatment groups two and three were told by the experiment facilitator that the NSF was not very effective (60%) in the same tasks.

The second manipulation, Information Warfare (IW), was operationalized in the form of an information manipulation resulting in two *spoofing* events. Spoofing is a tactic whereby the enemy has covertly gained access to the system and manipulates the track identity, such that a friendly aircraft appears on the display as an enemy and an enemy aircraft appears on the display as a friendly. Treatment groups three and four were subject to an information manipulation event during the simulation, while treatment groups one and two were not.

The location of each treatment group was counter-balanced across the four air space quadrants. The IW manipulation required the user to perceive an IW attack. The IW attack took the form of spoofing the identity of two tracks. To achieve the perception of the IW manipulation, the DDD software was modified so that if a user attacked a

friendly aircraft (to include a friendly aircraft spoofed as an enemy aircraft) an audible alarm would sound followed immediately by a pop-up window that displayed a warning message. This message indicated that the AWACS observed the destruction of a friendly aircraft (see Appendix 2). A mouse click action was required to end the audible signal and close the pop-up window. The act of ending this signal was used as an indication that the user perceived the IW spoofing manipulation. Manipulation checks were performed for the External Safeguard manipulation by means of a post-training multiple-choice test (see Appendix 5). The IW manipulation was checked through a computer generated log that recorded the subject's action of closing the alarm window following a fratricide incident.

The effectiveness of the manipulations was measured by two different methods. The effectiveness of the External Safeguard manipulation was measured by a post-training multiple-choice test (See Appendix 5, Multiple Choice Test). Three questions on this test measured different aspects of the External Safeguard entity in this experiment, the Network Security Forces (NSF). The effectiveness of the Information Warfare manipulation was measured both by the post-test multiple-choice test referred to above, as well as counting the number of spoofing acknowledgment messages sent by subjects who experienced the manipulation.

External Safeguard

Question 2 of the multiply choice test measured the subject's ability to recall the role of the NSF during the simulation. An examination of the test results showed 54 out

of 55 respondents answered the question correctly. The one subject who missed the question was provided immediate feedback and training on the role of the NSF.

Question 5 measured the subject's belief that the NSF is an external entity from the UCAV system. This check was important because the definition of an external safeguard given in Chapter II states that it is an organization, person, or object separate from the person or object of trust. An examination of the test results showed 37 out of 55 respondents answered the question correctly. Of the 18 subjects who missed the question, all but one answered the question that included the NSF as part of the UCAV system. The subjects who missed the question were provided immediate feedback and training on the UCAV system concept.

Question 11 measured the manipulation meant to set a level of effectiveness for the NSF. Out of the 23 subjects who were told the NSF was 90% effective, all 23 subjects answered the question on question correctly. Out of the 22 subjects who responded to the question and were told the NSF was 60% effective, 21 subjects answered the question correctly. The one subject who missed the question was provided immediate feedback and training on the effectiveness of the NSF.

Information Warfare

Question 4 of the multiple-choice test measured the subject's ability to recall the concept of Information Manipulation, or spoofing. Of the 55 subjects who responded, 42 subjects answered the question correctly. The other 12 subjects were provided immediate feedback and training on the concept of Information Manipulation.

The second means by which the Information Warfare manipulation was checked was to ensure the subjects who received a spoofing manipulation perceived the event. This measurement was achieved in two ways. First, an automatic pop-up window appeared on the subject's computer screen immediately following an attack against the spoofed track. The message stated that the track destroyed was actually a friendly aircraft. The subject was required to click on a button in order to proceed with the simulation. A check of the data logs showed that 20 of 20 subjects who destroyed the spoofed track acknowledged the pop-up window message. The second means by which this manipulation was measured was by a Request Information message sent by the subject to the experiment facilitator who was playing the role of an AWACS aircraft. Of the three subjects who suspected the spoofed track, all three subjects sent a request for information to the experiment facilitator and received a response that indicated the true identity of the track.

Hypothesis Measures

To review, a theoretical framework was presented in Chapter II and a set of hypotheses were developed that suggested the manipulation of external safeguards and IW in a military C2 environment will affect a user's trusting behavior (see Figure 8).

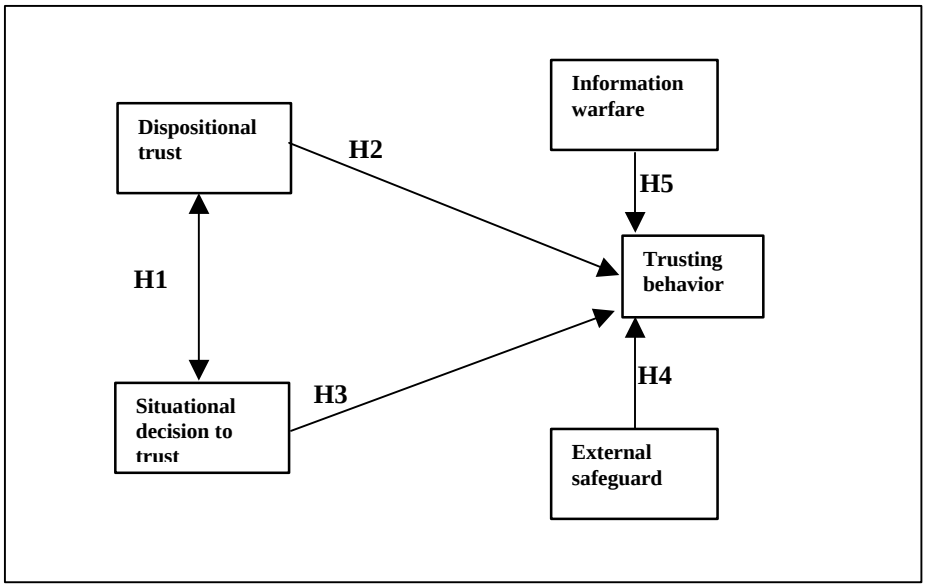


Figure 8. Adapted Model of Trust drawn from (McKnight and Chervaney,

Operationalized definitions of the two constructs, external safeguards and IW, were given in the Experiment Manipulation section of this chapter. In order to operationalize the other constructs of interest, clear and concise definitions for each were developed. These definitions were taken from McKnight and Chervany's model of trust (1999) and rewritten to reflect the specific objects of trust and situational context of this experiment.

Cognitive phenomena like "attitudes, motivations, expectations, intentions, and preferences cannot be observed" (Zikmund, 1984: 222). Therefore, a survey consisting item clusters that measured these attitudes was developed and administered before and after each experimental trial. The item clusters were developed based on the definitions of the constructs given in Table 2 (Chapter II) and adapted from self-reporting

measurements developed by McKnight and others to assess the subject's attitudes and beliefs. Dispositional trust and situational decision to trust were operationalized and measured through the use of a survey that employed a cluster of items using a five-point Likert-like scale (See Table 3 next page).

Trusting behavior was operationalized in terms of the user's action or inaction based on information received from the UCAV system. In this case, trusting behavior was measured by examining how many times the user requested identification verification from an external source (i.e. the AWACS participant) before taking an action or inaction. Therefore, the act of depending solely on the UCAV system (i.e. not contacting AWACS) is an indicator and measure of trusting behavior.

As mentioned in the previous chapter, note that the construct of intention to trust found in McKnight and Chervany's (1999) model of trust was not used in this study. In this experiment, the act of intending to trust is unique and different for each decision the subject makes about attacking or not attacking a track. Therefore, intention to trust could not be satisfactorily measured using a pre or post-experiment survey. In addition, if items were administered before each decision it is possible that the user may become aware of the true purpose of the experiment.

Table 3. Item Clusters

Construct: Dispositional trust (Faith in Technology's Competence)

Definition: The general tendency of users to believe in the technical competence of computer systems in general.

1a . My typical approach is to trust [new computer systems] until they prove I shouldn't trust them.

1b . I usually trust [computer systems] until they give me a reason not to trust them.

1c . I generally give [computer systems] the benefit of the doubt when I first [use] them.

Construct: Situational decision to trust

Definition: The extent to which a user intends to depend on an operational computer system in a real-world operational situation

2a . I feel I can depend on [computer systems] in [an operational context].

2b. [In an operational setting], I can depend on [computer systems] I work with.

2c. I can always rely on [computer systems] in an [operational setting].

2d. When I'm in [a operational environment], I feel I can rely on [the computer systems] I work with in that setting.

2e. I think I can adequately rely on the computer systems as tool in a operational setting.

Survey Design and Validation

The pre and post-experiment surveys were developed by employing a set of items that were developed to measure the constructs of dispositional trust – faith in technological competence and situational decision to trust. A set of three to five survey-type items was developed for each construct. A five-point Likert scale was used to measure user intentions, attitudes, and expectations. This scale ranged from 1(Strongly Disagree) on the left to 5 (Strongly Agree) on the right and 3 (Neutral in the middle). Subject experts were used to evaluate the items and ensure the items accurately measure the intended constructs. Items that were deemed not adequate measures of a construct were discarded.

The next step in evaluating the survey consisted of reliability and factor analysis. To accomplish this, all survey items were randomly listed on a survey form. This form was administered to the subjects. The results from the experiment were statistically analyzed. A factor analysis was performed to derive a correlation matrix and ensure the items loaded on the predicted number of factors. In addition, a reliability analysis was performed to derive reliability Coefficient alpha for the items. The reliability analysis produced an $\alpha >= .72$. This reliability level is sufficient for this type of study (Nunnally and Bernstein, 1994).

Data Analysis

Analysis of the data collected during the experimental trials was done through a variety of statistical analyses. A linear regression analysis was used to measure the

affects of constructs as a means to predict trusting behavior. This technique was used for hypotheses H2, H3, H4, and H5 as defined in Chapter II. In addition, a correlation analysis was performed to test H1.

Summary

This chapter described a research method to investigate the theorized relationship between external safeguards, information warfare, and trusting behavior. It described the experimental methodology, along with the operationalized constructs and a set of variables that were used to measure those operationalized constructs. Finally, this chapter described how the collected data was analyzed. Next, the results of the analysis are presented in Chapter IV. Chapter V describes a second experiment that was designed to validate the findings from the first experiment and to test the untested hypothesis from Chapter II. Chapter VI presents the results of the analysis for the second experiment. Finally, the interpretation and findings of both experiments, along with recommendations for future research efforts, are presented in Chapter VII.

IV. ANALYSIS OF DATA

(Experiment 1)

Data Analysis

This chapter presents an analysis of the data collected during the first experiment described in Chapter III. The results of this information in relation to the research hypotheses will be presented in Chapter VII. The following sections present the results of statistical analysis of the hypotheses under investigation in this experiment. A linear regression analysis was performed to determine what, if any effect each construct had in predicting the dependent variable, trusting behavior. A check for normality was performed on the dependent variable and the summary of this result can be found in Figure 10 on the next page. As described in Chapter III, trusting behavior was measured by counting the number of times the subject requested verification information from AWACS. Therefore, a low number of contacts indicates a high trusting behavior and a high number of contacts indicates a low trusting behavior. This type of count data results in a Poisson distribution which is, by definition, not normally distributed and was therefore transformed by taking the log of each count total. This log transformation resulted in a more normal distribution.

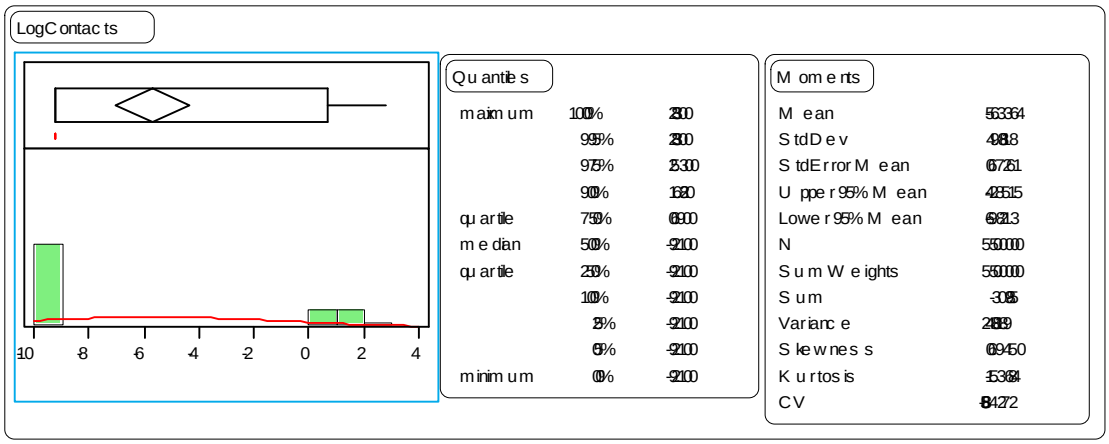


Figure 9 Descriptive Statistics of Trusting behavior Data

As can be seen from Figure 9, the distribution is not normal and indicates a high degree of kurtosis with a value of –1.53684. Kurtosis is a measure of the extent to which observations cluster around a central point. While the degree of the kurtosis was much higher than anticipated, kurtosis was expected given that the default behavior being measured was the act of not contacting AWACS. The violation of the assumption of normality and the high degree of kurtosis resulted in the need to perform a log-linear regression analysis on the data.

The log-linear regression analysis model consists of the following predictors: Constant, disposition to trust (DT), situational decision to trust (SDT), information warfare (IW), external safeguard (ES). The dependent variable was coded with either a 1 (AWACS contacted) or a 0 (AWACS not contact). A log-linear regression provides the odds of predicting the value of the dependent variable, as opposed to the probability of predicting the value of the dependent variable. A log-linear regression analysis begins with a model consisting of only the constant. The results of this model give the odds of predicting either AWACS was contacted or AWACS was not contacted at 65%. This

model was significant at the 0.050 level (df=1, p=.024). The next step in the log-linear regression analysis is to create a new model by adding the independent variables. The results of the second model show that by adding the independent variables, the odds of predicting the value of trusting behavior goes up to 78.2%. This means that the independent variables add some explanatory value to the model such that the odds of predicting trusting behavior increases by 13.2%. The summary statistics for this second model give a Cox & Snell R^2 = .323 and the Nagelkerke R^2 = .446.

Relationship Between Disposition to trust and Situational decision to trust (H1)

Hypothesis H1 predicts a positive correlation between disposition to trust and situational decision to trust. A review of the correlation analysis in Table 4 shows a significant positive correlation between disposition to trust and situational decision to trust at a significance level of $p < 0.001$. This finding supports Hypothesis 1 and

Table 4 Descriptive Statistics and Intercorrelations of Independent Variables

Correlations	M	SD	SDT	DT
SD	3.2764	.6583	1.000	**.372*** **
DT	3.8303	.5840	**.372*** **	1.000

* p < .10, ** p< .050, and *** p< .001

suggests that if a military commander trusts computers in general, they will also tend to trust computers in a command and control environment.

Relationship Between Disposition to trust and Trusting behavior (H2)

Hypothesis H2 predicted disposition to trust would have a positive effect on trusting behavior. The results from the regression analysis shown in Table 5 on the next page does not show disposition to trust to be significant (p = .401, β = -.574) at the 0.05

level. This finding does not support Hypothesis 2 which suggests that a military commander's trust of computers in general is a useful predictor of their willingness to trust information presented to them on a C2 information system.

Table 5 Log-linear Regression Analysis Summary of IW, ES, SDT, and DT as Determinants of Trusting Behavior

		b	S.E.	Wald	df	p
Step 1	**IW**	-9.455	42.058	.051	1	.822
	ES	.127	.852	.022	1	.881
	DT	-.574	.684	.706	1	.401
	SDT	-1.084	.596	3.311	1	.069
	Constant	5.099	2.826	3.257	1	.071

a Variable(s) entered on step 1: IW, ST, IW_ST, DSFT, SD.

Relationship Between Situational decision to trust and Trusting behavior (H3)

Hypothesis H3 predicted situational decision to trust would have a positive effect on trusting behavior. The results from the regression analysis shown in Table 5 above shows situational decision to trust to be marginally significant ($p = .069$, $\beta = -1.084$) at the 0.05 level. This finding support Hypothesis 3 which suggests that a military commander's trust in computers in a C2 environment is a useful predictor of their willingness to trust information presented on a C2 information system.

Effect of External Safeguards on Trusting behavior (H4)

Hypothesis H4 predicted external safeguards would have a positive effect on trusting behavior. The results from the regression analysis (see Table 5 above) show external safeguards to be significant ($p = .881$, $\beta = .127$) at the 0.05 level. Therefore, these findings offer no support for Hypothesis 4 which suggested a commander's belief

in the effectiveness of an external safeguard to a C2 information system would have a positive effect on their willingness to trust information presented on the C2 information system.

Effect of Information Warfare on Trusting behavior (H5)

Hypothesis H5 predicted information warfare would have a negative effect on trusting behavior. The results from the regression analysis (see Table 5 above) shows information warfare not significant ($p = .882$, $\beta = -9.455$) at the 0.05 level. Therefore, there is no evidence to support Hypothesis 5 which suggests that the perceived presence of an information warfare attack, such as the manipulation of air track data, has a negative effect on a military commanders willingness to trust the information received from a C2 information system.

Conclusion

The violation of the assumption of normality for the trusting behavior data prompted the use of log-linear regression analysis to determine if any of the independent variables would increase the odds of predicting trusting behavior. Of the four independent variables tested in this model, only situational decision to trust was a significant predictor of trusting behavior. However, the correlation analysis between situational decision to trust and dispositional trust was also significant and supported hypothesis H1.

The problem with the normality of trusting behavior led to a review of the experimental design in order to identify possible causes. This review identified several possible causes for this problem and revealed some possible new problems. Discussions

with some of the subjects following the experiment indicate that they were so busy concentrating on performing the required tasks (i.e. moving aircraft, attacking, refueling, returning to base, identifying tracks, etc) that they either did not have time to contact AWACS for verification or had forgotten about the option to contact AWACS. This may have resulted in the low number of contacts made with AWACS. Another possible problem with the experimental design may have been the timing of the survey questions. It is possible that bias was introduced by administering situational decision to trust and dispositional trust questions together on the same survey and following the training on the UCAV system. The statements made during the training about the effectiveness of the UCAV system may have biased the subject's responses with regard to computers in general.. Therefore, a second experiment was designed to validate the findings from the first experiment and eliminate the possible problems identified above. The next chapter describes the second experiment and its design.

V. METHODOLOGY

(Experiment 2)

Overview

As discussed briefly in the previous chapter, the methodology used in first experiment may have resulted in experimental effects (e.g. task saturation). Additionally, the metric used to measure trusting behavior may not have been robust enough to study the research hypotheses. Finally, the timing of the survey instruments may have introduced bias into the experiment. Therefore, a second experiment was designed with the same basic goals as the first.

This chapter describes the second experiment, which tested the same hypotheses described as presented in Chapter II. It operationalizes each construct of interest by applying the same theoretical framework and defining a modified set of variables that were used to measure these constructs. Finally, the data collection process is described, along with the statistical methods used to analyze and make inference about the data.

Experimental Design

A similar military command and control (C2) scenario was developed for use with the same high-fidelity computer simulator used in the first experiment. This was done in order to allow for easier comparison of results between the two experiments. This experiment collected quantitative measures of subject behaviors over the course of each experimental trial, as well as measurable attitudes and beliefs through a pre and post survey questionnaire in the same basic fashion as the first experiment. This experiment

maintained the same between group design as the first experiment in which the same two independent variables were manipulated. These variables were completely crossed to a 2 X 2-design configuration as seen in Figure 10. Each subject experienced only one of the four possible conditions. The trials were counter-balanced in order to ensure a random ordering of the trials.

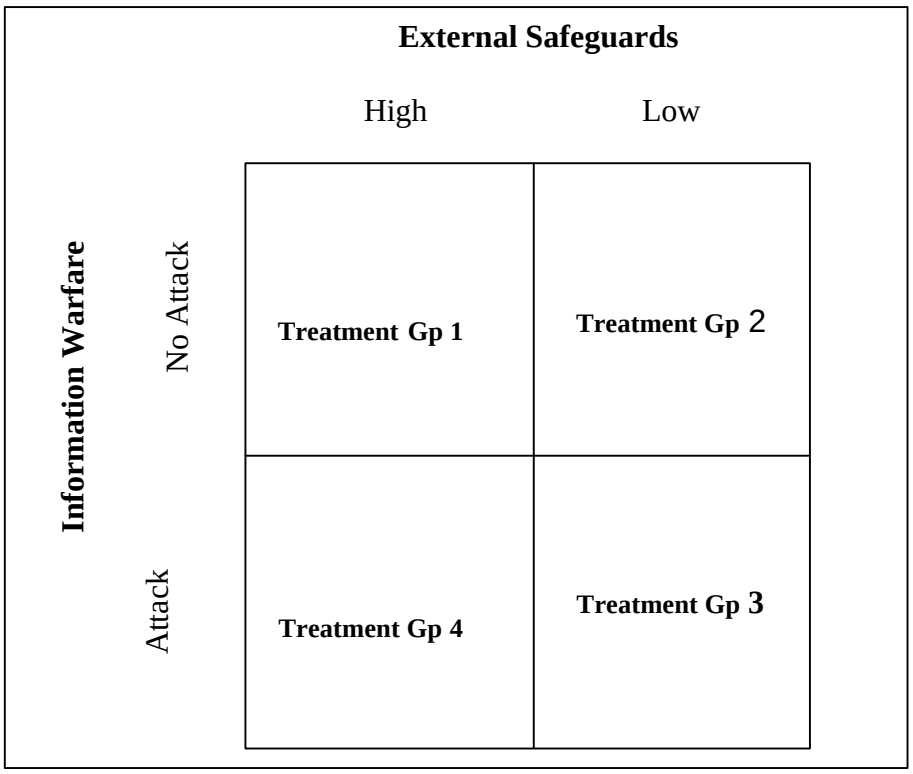


Figure 10. Group Configurations

Each subject was given training on the weapon system concept and computer interface. A further description of the training is described in the Tasks and Procedures section of this chapter. Following training, each subject was tasked by the experiment administrator (acting as an Air Force Research Laboratory field evaluator and reading from a script) to perform a hidden-profile, decision-making task that involved the control

of multiple fixed Surface-to-Air Missiles (SAM) sites and radar sites to defend a designated air space on the computer display (see Appendix 13). Control of each SAM site was performed through various user actions on the DDD system. Subjects were told the SAM sites and radar sites were part of a deployed operational Air Defense Unit (ADU) were under their direct control.

Subjects were tasked to identify incoming air tracks by comparing the icon information from the graphical display with a list of automated electronic messages sent by the radar sites. If the air track was identified and confirmed by the subject as a hostile, they were authorized to attack the target using one of their SAM sites. Subjects were told the objective of their mission was to stop all hostile tracks before they entered protected airspace. Subjects were further told that the while the computer system would automatically determine the identity of all air tracks, it was possible for the automated messages sent to the computer system to be manipulated by the enemy. The number of tasks required to perform their mission were substantially reduced in this experiment in order to reduce the potential problem of task saturation observed in the first experiment.

Unlike the first experiment where the IW threat and network defender were simulated, the experiment administrator introduced two people to the subjects. This was done following the introduction part of the training. Subjects were told these two people would be playing the role of the network attacker and the other as network defender. Subjects were then told these individuals would be located in the next room where they would perform their tasks. The experiment administrator instructed the subjects that they should expect to receive electronic messages from the network defender if he or she detected a network attack by the attacker. In actuality, both of these people were

portraying the role of subjects. Following this explanation, these two people left the room and performed no further part in the experiment. As in the first experiment, the IW spoofing attacks were scripted into the scenario. This change was made in order to strengthen the salience of the IW and external safeguard manipulations.

Also unlike the first experiment, subjects were not given a means to contact another party in order to confirm the identity of the tracks. Recall that the contact of the outside party (AWAC) was used in the first experiment as the measure of trusting behavior. Due to the problems identified in the last chapter with this measure (i.e. the measure resulted in only one or two states: contacted or not contracted), a more robust and descriptive measure was developed for this experiment.

This new measure was collected by requiring subjects to set a confidence level for each hostile track before initiating an attack. The confidence level was a scale from 1 to 5, where 1 represented very low confidence in the track identity and 5 represented very high confidence in the track identity. This confidence level was also tied to the scoring system so that points were calculated as a function of confidence level. Points were received when tracks were correctly assessed and points subtracted when tracks were incorrectly assessed.

As in the first experiment, all subjects received a threat message from the network defender, the Network Security Force (NSF), approximately five minutes into the simulation. This message indicated an attempted attack against the network had occurred (see Appendix 14). Following this message, four spoofed tracks would appear for subjects receiving the IW manipulation. These tracks were depicted graphically and by electronic message as hostile aircraft when; in fact, they were friendly aircraft. If the

subjects destroyed the friendly aircraft, a visual and audible alarm was triggered indicating a fratricide had occurred. In addition, subjects were able to perceive this error by observing the loss of points to their defensive score.

To give the experimental task a sense of realism and urgency, a scenario briefing was provided to each subject to read before the start of the experimental trial (see Appendix 15). The scenario briefing laid out a realistic military threat environment in which an imminent attack by enemy aircraft was expected. Then the experiment facilitator explained the scoring system (see Appendix 16) used during the simulation. As mentioned earlier, the scoring system was tied to the confidence level assignments and was designed to simulate the high-risk environment of combat operations. Subjects were told their overall score would be used to determine the success of the mission.

Pilot Study

A pilot study using Air Force Company Grade Officers (Ss =10) was performed to ensure the experiment was feasible, safe, and met the stated objectives. This test helped ensure problems identified in the first experiment did not reoccur and new problems with subject reactivity and game play were not introduced.

Findings from the pilot study resulted in a reduction in the number of air tracks from 48 in the first experiment to 23 in this experiment. Additionally, post-interviews with the pilot study subjects were used to gage the perceived level of task saturation. Findings from these post-interviews found that subjects were comfortable with the speed of the game and task workload. This was important given the observations from the first experiment where it is possible that task saturation errors may have occurred (Brehmer

and Dorner, 1993). Recall that Brehmer and Dorner (1993) defines task saturation as overwhelming the subjects with too many assigned tasks to perform. This type of error could result in the measurement of something other than the intended measure. Finally, a post-hoc analysis of the pilot study data was performed to ensure no violation of normality was present in the new measure for trusting behavior (i.e. confidence ratings of 1 to 5). This analysis showed the confidence level data were normally distributed.

Subjects

A sample (Ss=38) of Air Force officers were recruited from the Air War College and Aerospace Basic Course at Maxwell Air Force Base (AFB), Alabama and from the Air Force Institute of Technology at Wright-Patterson AFB, Ohio to participate in this study. The ages of subjects ranged from 24 to 56 years old and their military ranks ranged from Second Lieutenant to Colonel.

Equipment and Facilities

All experiment sessions were run in a conference room with a single entrance. Each subject performed his or her tasks in an individual workspace around a conference table. While each subject could not visually see another subject's computer display, their proximity to each other could have resulted in their hearing each other's comments. Therefore, each subject was told that a communications blackout was in effect. Each subject's workspace consisted of a chair, a desk surface, a PC-type laptop computer system loaded with a Linux operating system and DDD software, and quick reference sheets that defined icons and scoring information. The room was also equipped with a desktop PC-type computer with overhead projection capabilities and setup to run

Microsoft's PowerPoint application. These items were used during the training portion of the experimental trial.

Tasks and Procedures

Three experimental trials were scheduled each day at Maxwell AFB, Alabama and one to three trials each day for Wright-Patterson AFB, Ohio. Each scheduled session had between one and four subjects. Each trial lasted approximately one and half-hours (see Figure 11). The experiment ran for five consecutive days at Maxwell AFB, Alabama and resulted in 32 experimental trials. The remaining eight experimental trials were run at Wright-Patterson AFB, Ohio over a period of two weeks. Treatments were randomly assigned by means of a randomized block design (see Appendix 17).

On the scheduled test day, subjects were instructed to report to the evaluation room. Subjects were assigned a workspace position based on the order in which they

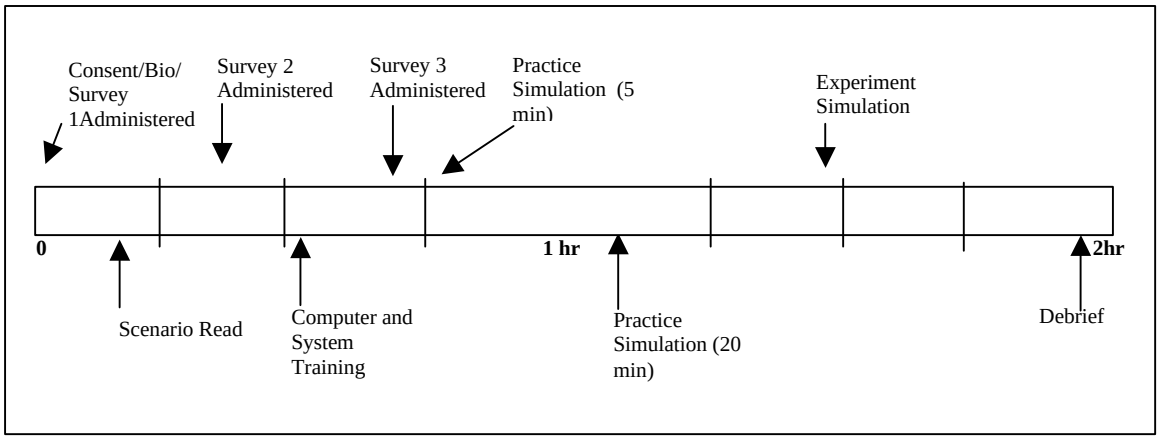


Figure 11 Experimental Time-line (Experiment 2)

arrived and were instructed to sign a log-in sheet. An introductory package was provided to each subject. The package included a standard consent form, a biometric data collection form, and survey 1 (see Appendix 18, 19, and 20). Subjects were asked to fill-out each form before the start of the experimental trial.

The experiment facilitator (reading from a script) started the trial by giving a brief explanation of the experiment. The experiment facilitator then instructed subjects to read along with the scenario brief while the facilitator read it out load. Following the scenario briefing, the experiment facilitator answered any questions and then instructed subjects to complete survey 2 (see Appendix 21). Once the surveys were complete, the experiment facilitator went through a PowerPoint training presentation on the desktop PC located in the room (see Appendix 22). Following the training, each subject was given an opportunity to ask questions. Subjects were then instructed to complete survey 3 (see Appendix 23). The subjects were then instructed to take their place at their stations. The experiment facilitator instructed each subject to begin the training simulation by clicking the Start button. Subjects were individually shown how to perform the various functions needed to operate the system. The experiment facilitators freely answered questions. This first hands-on session lasted approximately five minutes. Following this session, one of the experiment facilitators briefed the subjects on the training mission scenario, while the other facilitator prepared the computers for the next session. Once the briefing was complete, subjects participated in a 20-minute training simulation session. Again, the experiment facilitators provided assistance to subjects on system operation and game play rules.

Following the training session, subjects were reminded that the two people posing as subjects would be participating in the next room. Subjects were then told the effectiveness of the experiment assistant posing as the network defender. This effectiveness was either 97% effective in detecting enemy information warfare attacks and defending the network or 57% effective depending on the external safeguard manipulation the subject received. These levels were increased slightly from the first experiment for the effective manipulation and decreased slightly for the ineffective manipulation in order an attempt to strengthen the manipulation. Once all subjects indicated they were ready to begin, the subjects were instructed to start the simulation. Subjects were instructed to raise their hands to request assistance if they encountered a computer malfunction or procedural question. Finally, subjects were instructed to remain at their workstation at the completion of the experiment until otherwise directed by the experiment facilitator.

When the simulation ended, one of the experiment facilitators saved the recorded data logs onto floppy disks. The other experiment administrator revealed the true purpose of the experiment. An informal question and answer session was conducted at that time. It was interesting to note that nearly all of the subjects confessed that they believed there were actual people trying to attack and defend the network from the other room.

Experiment Manipulations

The experiment manipulations were the same as in the first experiment. The first experiment manipulation was the construct called External Safeguards. External

Safeguards was operationalized in the form of the experiment assistant posing as the game participant called the Network Security Force (NSF). The NSF was described as an external agency that was not actually part of the ADU. As in the first experiment, this was done to ensure the subjects could separate the NSF from the ADU system. Subjects were told that the NSF's role was to monitor and protect the LAN against IW attacks. The NSF was, in essence, an external safeguard that contributed to the subject's sense of normality and confidence by providing alerts to the subjects of IW attacks. Treatment groups one and four were told by the experiment facilitator that the NSF was very effective (97%) in detecting enemy information attacks and defending the network. Treatment groups two and three were told by the experiment facilitator that the NSF was not very effective (57%) in the same tasks.

The second manipulation, IW, was operationalized in the form of an information manipulation resulting in *spoofing* events. Recall that spoofing is a tactic whereby the enemy has covertly gained access to the system and manipulates the track identity, such that a friendly aircraft appears on the display as an enemy. Treatment groups three and four were subject to four information manipulation events during the simulation, while treatment groups one and two received none. The number of spoofing events was increased from the two in the first experiment to four in the second experiment in order to strengthen this manipulation.

The IW manipulation required the user to perceive an IW attack. To achieve the perception of the IW manipulation, the DDD software was modified so that if a user attacked a friendly aircraft (to include a friendly aircraft spoofed as an enemy aircraft) an audible alarm would sound followed immediately by a pop-up window that displayed a

warning message. This message indicated that the Air Operation Center (AOC) observed the destruction of a friendly aircraft (see Appendix 24). A mouse click action was required to end the audible signal and close the pop-up window. The act of canceling this signal was used as an indication that the user perceived the IW spoofing manipulation.

External Safeguard

The multiple-choice test from the first experiment was modified slightly and used in the second experiment to measure the effectiveness of the two manipulations. Unfortunately, the question that checked to see if the subjects were able to recall the effectiveness of the NSF was accidentally omitted. Question 1 of the multiply choice test measured the subject's ability to recall the role of the NSF during the simulation. An examination of the test results showed 38 out of 38 respondents answered the question correctly. Question 4 measured the subject's ability to exclude including the NSF from the UCAV system concept. This question establishes the concept of the NSF being an external entity. An examination of the test results showed 38 out of 38 respondents answered the question correctly.

Information Warfare

The same check used to check the IW manipulation in the first experiment were used in the second experiment. Question 3 of the multiple-choice test measured the subject's ability to recall the concept of Information Manipulation, or spoofing. Of the 38 subjects who responded, 36 subjects answered the question correctly.

The second means by which the Information Warfare manipulation was checked was to ensure the subjects who received a spoofing manipulation perceived the event.

This measurement was achieved in two ways. First, an automatic pop-up window appeared on the subject's computer screen immediately following an attack against the spoofed track. The messaged stated that the track destroyed was actually a friendly aircraft. The subject was required to click on a button in order to proceed with the simulation. A check of the data logs showed that 20 of 20 subjects who destroyed the spoofed track acknowledged the pop-up window message.

Hypothesis Measures

To review, a theoretical framework was presented in Chapter II and a set of hypotheses were developed that suggested the manipulation of External Safeguards and Information Warfare in a military C2 environment will affect a user's Trusting Behavior (see Figure 12 below). Operationalized definitions of the two constructs, External Safeguards and Information Warfare, were given in the Experiment Manipulation section of this chapter. The operationalization of these constructs was the same as described in Chapter III.

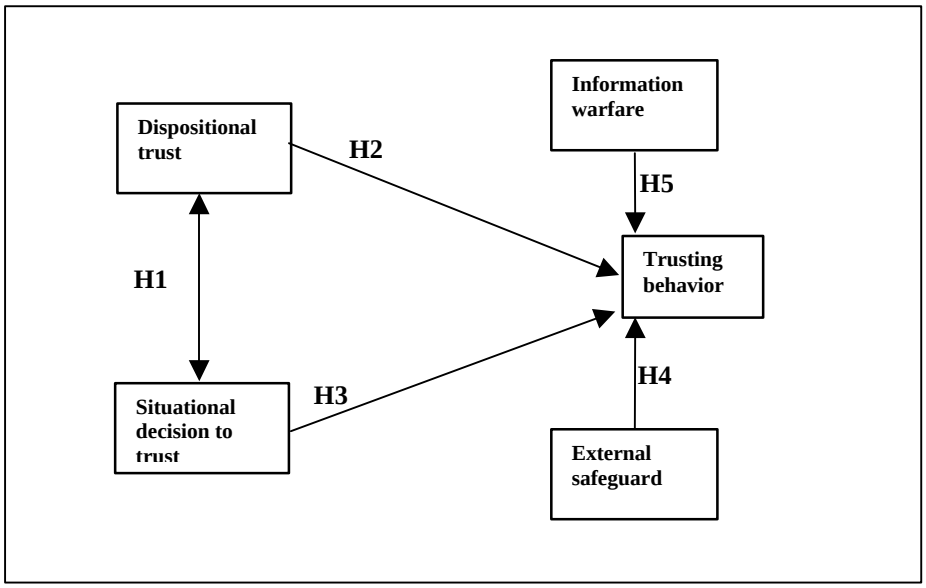


Figure 12. Adapted Model of Trust drawn from (McKnight and Chervaney,

Cognitive phenomena like “attitudes, motivations, expectations, intentions, and preferences cannot be observed” (Zikmund, 1984: 222). Therefore, a survey consisting item clusters that measured these attitudes was developed and administered during the experimental trial. However, Chapter IV suggested that the survey used to collect attitudinal measures for the constructs of dispositional trust and situational decision may have resulted in bias. Therefore, a separate survey was created for each construct and administered in the order shown in Figure 12 on the previous page. Additionally, a new survey was created in an attempt to measure the construct of trusting belief. The item clusters were developed based on the definitions of the constructs given in Table 9 and adapted from the same or similar self-reporting measurements developed by McKnight and others and that were used in the first experiment.

Table 6. Item Clusters

Construct: Dispositional Trust (Faith in Technology's Competence)

Definition: The general tendency of users to believe in the technical competence of computer systems in general.

1a. If you initiate a task for the average computer system to perform, the computer system will finish it correctly.

1b. I believe that most computer systems are consistent.

1c. Most computer systems are reliable.

1d. I believe that most computer systems are technically competent.

1e. I feel I can depend on most computer systems.

1f. I can trust most computer systems.

Construct: Situational Decision to Trust

Definition: The extent to which a user intends to depend on an operational computer system in a real-world operational situation

2a. In a command and control environment like described in the scenario brief, I believe computers can be relied upon to help commanders make operational decisions.

2b. I feel I can depend on computer systems to provide timely and accurate information to battle commanders in a combat situation.

2c. In a command and control setting like the one described in the scenario, I feel that I can adequately trust information received from most computer systems.

2d. I believe that most computer systems used in deployable battle cabs are secure enough to trust in combat situations.

2e. I feel most computer systems used in command and control units are dependable.

Table 6. Item Clusters (Continued)

Construct: Trusting Belief

Definition: The extent to which a user believes and has confidence in a specific person or object.

3a. The DDD computer system is predictable.

3b. The DDD computer system is consistent.

3c. The DDD computer system is technically competent.

3d The DDD computer system has integrity.

3e. The DDD computer system is reliable.

3f. The DDD computer system is dependable

3g. I can trust the DDD computer system.

Dispositional trust, situational decision to trust, and trusting belief were each operationalized and measured through the use of a separate survey that employed a cluster of items using a seven-point Likert-like scale. Note that the scale was changed from a five-point scale in the first experiment in order to increase the sensitivity of the measures.

Trusting Behavior was operationalized in terms of the confidence-level they assigned to each hostile track. Confidence levels have been used in other research as a measure of trust (Bisantz, Ann M., James Llinas, Younho Seong, Richard Finger, and Jiun-Yin Jian, 2000).

Survey Design

The surveys employed a set of items that were developed to measure the constructs of dispositional trust – faith in technological competence, situational decision to trust, and trusting belief. A set of three to five survey-type items was developed for each construct. A seven-point Likert scale was used to measure user intentions, attitudes, and expectations. This scale ranged from 1(Strongly Disagree) on the left to 7 (Strongly Agree) on the right and 4 (Neutral in the middle). As in the first experiment, a reliability analysis was performed to derive the reliability for the items. The reliability analysis produced an $\alpha >= .67$. While not as strong as what was found in the first experiment, the reliability of the series are sufficient for this type of study (Nunnally and Bernstein, 1994).

Data Analysis

Analysis of the data collected during the experimental trials was done using the same statistical methods in Chapter IV. All of the following tests were performed on the experiment data to evaluate each of the hypotheses proposed in Chapter II. A linear regression analysis was used to measure the affects of constructs as a means to predict trusting behavior. This technique was used for hypotheses H2, H3, H4, and H5 as defined in Chapter II. In addition, a correlation analysis was performed to test H1 and a linear regression analysis was again used to examine the effects of each construct on the dependent variable, trusting behavior.

Summary

This chapter described a research method to investigate the research problem and hypotheses presented in Chapter II. It described the experimental methodology, along with the operationalized constructs and a set of variables that were used to measure those operationalized constructs and compared these to the first experimental methodology used for the first experiment. Finally, this chapter described how the collected data was analyzed. The results of the analysis described in this chapter are described in Chapter VI. Chapter VII interprets and findings of experiments, the limitations of both, and recommendations for future research efforts.

VI. ANALYSIS OF DATA

(Experiment 2)

Data Analysis

This chapter presents an analysis of the data collected during the second experiment as described in Chapter V. The results of this information in relation to the research hypotheses will be compared with the result from Chapter IV in Chapter VII. The following sections present the results of statistical analysis of the hypotheses under investigation in this experiment. A linear regression analysis was performed to determine what, if any effect each construct had in predicting the dependent variable, trusting behavior. A check for normality was performed on the dependent variable and the summary of this result can be found in Figure 14 on the next page.

As described in Chapter V, trusting behavior was measured by the confidence level given to each track prior to a decision. As can be seen from Figure 14, while the distribution of this data is normal, the graph is skewed to the right with a value of –1.812. The degree of the skewness was anticipated given that the score system was tied to the confidence level. In other words, the higher the confidence level the higher the score if the decision was correct. Additionally, the higher the confidence level the greater the decrement to the score if the decision is wrong. Von Neumann's game theory suggests that rational people will use strategies to maximize their utility (Von Neumann, J. & Morgenstern, 1944). In this case, the utility is the score, therefore the number of assigned confidence levels would, according to game theory, be generally higher.

The regression analysis model consists of the following predictors: Constant, disposition to trust, situational decision to trust, disposition to trust * situational decision to trust, information warfare, and external safeguard. The dependent variable was the mean confidence level over the course of the experiment.

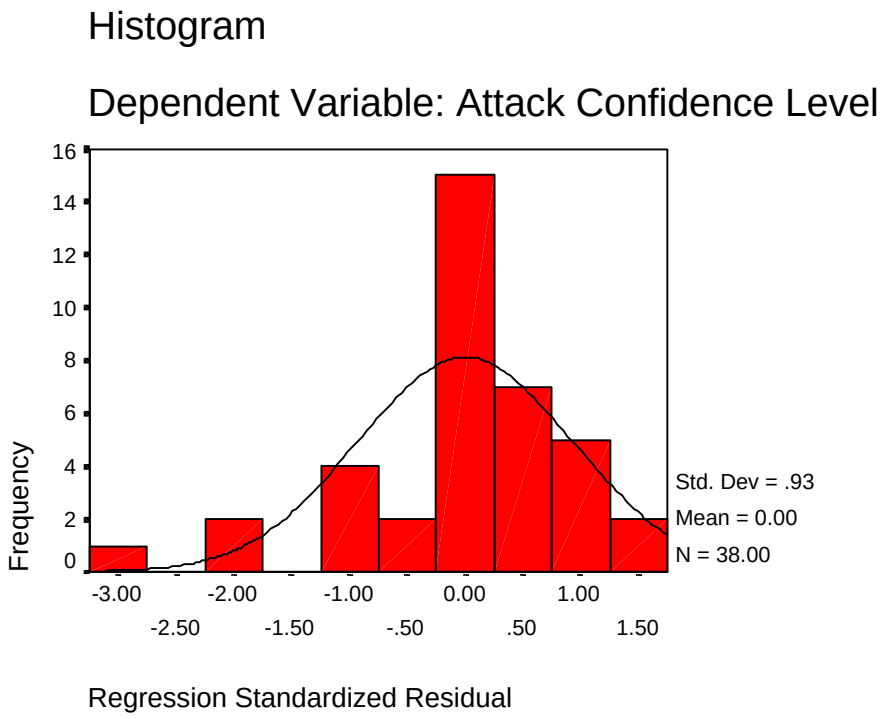


Figure 13. Trusting Behavior Normality Analysis

The regression analysis model consists of the same predictors as used in the Chapter IV regression model: Constant, disposition to trust (DT), situational decision to trust (SDT), information warfare (IW), and external safeguard (ES). However, the dependent variable used in this model was the confidence level assigned to each air track by the subject prior to making a decision (i.e. trusting behavior). The results from the

regression analysis show the model to be significant at the 0.050 level (df=4, F=2.788, p=0.042).

Relationship Between Disposition to trust and Situational decision to trust (H1)

Hypothesis H1 predicts a positive correlation between disposition to trust and situational decision to trust. A review of the correlation analysis in Table 7 below shows a significant positive correlation at a significance level of p<0.01 level (1-tailed) between a subject's disposition to trust computers in and their situational decision to trust computers in a specific situation. This finding supports Hypothesis 1 and suggests that if a military commander trusts computers in general, they will also tend to trust computers in a command and control environment.

Table 7 Descriptive Statistics and Intercorrelations of Independent Variables

Correlations	M	SD	SDT	DT
SD	4.8579	.8278	1.000	**.603*** **
DT	5.3421	.7323	**.603*** **	1.000

* p< .10, ** p< .050, and *** p< .001

Relationship Between Disposition to trust and Trusting behavior (H2)

Hypothesis H2 predicted disposition to trust would have a positive effect on trusting behavior. The results from the regression analysis shown in Table 8 on the next page shows disposition to trust to not be significant (p = ..761, β = .060) at the 0.05 level of significance. This finding does not support Hypothesis 2 which suggests that a military commander's trust of computers in general is a useful predictor of their willingness to trust information presented to them on a C2 information system.

Table 8 Regression Analysis Summary of IW, ES, SDT, DT, and DT*SDT as Determinants of Trusting Behavior

	Experiment 2 (Maxwell AFB)			
	R^2	**DR^2**	b	**Significance**
	.253	.162		
IW			..007	
ES			**-.282**	*
SDT			**.353**	*****
DT			.060	

* p< .10, ** p< .050, and *** p< .001

Relationship Between Situational decision to trust and Trusting behavior (H3)

Hypothesis H3 predicted situational decision to trust would have a positive effect on trusting behavior. The results from the regression analysis shown in Table 8 above shows situational decision to trust to be marginally significant ($p = .076$, $\beta = .353$) at the 0.05 level of significance. This finding supports Hypothesis 3 which suggests that a military commander's trust in computers in a C2 environment is a useful predictor of their willingness to trust information presented to them on a C2 information system.

Effect of External Safeguards on Trusting behavior (H4)

Hypothesis H4 predicted external safeguards would have a positive effect on trusting behavior. The results from the regression analysis shows external safeguards is marginally significant ($p = .077$, $\beta = -.282$) at the 0.05 level of significance. However, the beta coefficient is the opposite from what was predicted in Hypothesis 4. That is to say, while there is no evidence to support the hypothesis that a military commander's belief in the effectiveness of an external safeguard is a useful predictor of their

willingness to trust information presented to them on a C2 information system, there does appear to be some suggestion that the opposite may be true.

Effect of Information Warfare on Trusting behavior (H5)

Hypothesis H5 predicted information warfare would have a negative effect on trusting behavior. The results from the regression analysis shown in Table 8 above shows information warfare not to be significant ($p = .965$, $\beta = .007$) at the 0.05 level of significance. Therefore, there is no evidence to support Hypothesis 5 which suggests that the perceived presence of an information warfare attack, such as the manipulation of air track data, has a negative effect on a military commander's willingness to trust the information received from a C2 information system.

Conclusion

The findings from this data analysis show some significant results and are discussed in the next chapter concerning the experimental hypotheses. Additionally, the results from the first and second experiment will be compared and discussed in Chapter VII. Finally, Chapter VII will present some limitations of each experiment and offer some suggestions for follow-on research.

VII. FINDINGS

Introduction

This chapter examines the findings from the data analyses from the two experiments with respect to the research hypotheses offered in Chapter II. Next, limitations of the research experiments are discussed. Finally, proposals are offered for further research. The research question for this study was what affect external safeguards has on human-information systems trust in an information warfare domain. Five hypotheses were developed in Chapter II and tested in the two experiments described in Chapters 3 and 5. The conclusions of each of these research questions are presented below:

Dispositional trust and situational decision to trust are positively correlated (H1)

The findings from the first experiment showed a significant positive correlation between dispositional trust and situational decision to trust ($p = .003$, Pearson Correlation = .372). The second experiment supported this finding with a significant positive correlation ($p = .000$, Pearson Correlation = .603). While this relationship is not shown in McKnight and Chervany's (1999) model of trust, it is consistent with the definitions given in their model and with that of this study. Remember that dispositional trust was defined in this study as a general tendency to trust computers, while situational decision to trust was defined as a tendency to trust computer is specific situations. The increase in the correlation values from the first experiment to the second experiment may be due to the modified question sets used in the second experiment. Despite this, the

correlation results from both experiments suggest that if a military commander has a general tendency to trust computers, then he or she would also have a tendency to trust them in command and control situations.

Disposition to trust will have a positive effect on trusting behavior (H2)

Results from the first experiment showed dispositional trust to be not significant in the linear regression analysis ($p = .401$, $\beta = -.574$) at the .05 level. The second experiment also showed no significant effect at the 0.05 level ($p = .307$, $\beta = .060$). These findings were inconsistent with both McKnight and Chervany's (1999) model of trust and the model presented in this paper. The failure of this facet of trust to show a significant effect on trusting behavior seems to indicate that while a military commander may trust computers in general, this trust does not carry over into the C2 environment.

Situational decision to trust will positively affect trusting behavior (H3)

The analysis of the data from the first experiment showed situational decision to trust to have a significant effect on the regression model ($p = .069$, $\beta = -1.084$) at the 0.1 level. Likewise, the second experiment showed a significant positive effect ($p = .076$, $\beta = .309$) at the 0.1 level. The findings of these two experiments are consistent with McKnight and Chervany's model of trust and the model presented in Chapter II. These findings suggest that a military commander's trust in computers in a C2 environment is a good predictor of their trusting behavior. This is consistent with the OODA Loop model of decision-making which suggests that when a military commander is orienting information into possible courses of action, they try to match the current situation with

their past experience in similar situation (Boyd, 1987). In order words, the situational context of using computers is a good predictor of trusting behavior.

External safeguards have a positive effect on trusting behavior (H4)

The analysis from the first experiment showed no significant negative effect in the regression model ($p = .881$, $\beta = .127$. However, the analysis from the second experiment did find a significant effect on the regression model ($p = .077$, $\beta = -.406$), but showed an unexpected negative effect in the beta coefficient. External safeguard was operationalized the same way in the first and second experiment with only one difference. In the first experiment, the subjects were told the external safeguard was simulated by a computer with a programmed effectiveness rate (i.e. either 90% effective in protecting the network or 60% effective). Subjects in the second experiment were introduced to a person posing as the external safeguard and were told that the person had an effectiveness rating (i.e. either 97% effective in protecting the network or 57% effective) that was achieved during the practice session of the experiment. The significant negative effect found in the second experiment suggests that groups who were told the person protecting the network was highly effective tended to assign lower confidence levels than those who were told the person was not effective.

The unexpected negative effects from these two experiments may be explained in part by the affect of unfulfilled expectations. Muir (1994) describes trust as the expected or predicted behavior by a person or object. This expectation is developed over time by observations of actual behavior. Therefore, when a subject saw a hostile track on the computer display, shot it down, and received positive feedback, the subject's expectation

of future information received from the computer display continued to be positive. However, if the subject's expectations were unfulfilled by the computer system, it is likely that the subject would tend to be distrusting of future information received from the computer display. This affect of unfulfilled expectations may be have been strong enough and lasted long enough to account for the unexpected correlation findings. This is what was observed in Muir's (1994) research and supported in other research (Szoyna and Scommell, 1993).

Additionally, the failure of this manipulation to show a significant effect on the regression model in the first experiment may be due to an additional factor. As mentioned at the end of Chapter IV, the first experiment may have introduced too many tasks for the subjects to perform and resulted in an experimental anomaly called task saturation (Brehmer and Dorner, 1993). If the subjects were over tasked, it is possible that their failure to contact AWACS may be a result of spending too much time on the air defense task and forgetting about the option to contact AWACS.

Information warfare has a negative effect on trusting behavior (H5)

The analysis from the first experiment found no significant negative effect between information warfare and trusting behavior ($p = .882$, $\beta = -9.455$). The analysis from the second experiment also found no significant effect ($p = ..965$, $\beta = .007$). In other words, it appears that a perceived information warfare attack had no effect on a military commander's trusting behavior in a C2 environment. There are two possible explanations for this finding. Moray and Lee (1996) suggest that a person's confidence in their own ability to manually control automation may be a factor for predicting trusting

behavior. Therefore, it is possible that subjects who were self-confident with their ability to detect erroneous track information during the training scenario may have been demonstrated more trusting behaviors. Unfortunately, self-confidence and computer proficiency were not measured in this experiment.

Another possible explanation for this opposite finding may be due to the effects of game theory (Von Neumann, J. & Morgenstern, 1944). Game theorists suggest, similar to the rational decision making model that people will use the available information to adjust their strategy in order to maximize utility (Simon, 1957; Hall, 1996). Since the measure of trusting behavior in the second experiment was assigned confidence levels, and since those confidence levels were tied to the scoring system, it is possible that some subjects disregarded instructions to treat the simulation like a real-world situation and instead assigned confidence levels in such a way as to maximize their score. A similar scoring system was also used in the first experiment, except there was a penalty given if subjects contacted AWACS for confirmation.

Research Finding Overview

As predicted, there is evidence to suggest that a military commander's disposition to trust computers in general is positively correlated with their situational decision to trust computers. Despite this correlation, only situational decision to trust seems to have been a good predictor of trusting behavior in a C2 environment. Therefore, if a C2 unit wants to decrease the time for its military commanders to make decisions, they should develop a method to foster the commander's trust in the C2 information system. However, if the

unit wants to increase skepticism in the systems that deliver information, they should develop a method to break-down the commander's trust in these systems.

There also appears to be some evidence to suggest that trust an external safeguard may be a good predictor of trusting behavior in a C2 environment. However, this study found that external safeguards had a negative effect on trusting behavior. As discussed earlier, this may be a result of the military commander's unfulfilled expectations of the safeguard. This finding suggests that C2 units who want to lessen this negative effect may want develop a method that creates doubt about the effectiveness of safeguards.

Research Limitations

The subject populations for both experiments were active duty Air Force personnel. The population of the first experiment was actually a subgroup to this population, Air Battle Managers. Air Battle Managers are familiar with real-world command and control situations, since that is the focus of their primary mission. However, the affects from the first experiment may have proved stronger if the scenario were run using an AWACS simulator. Since no AWACS simulator was available for this experiment, another command and control simulator was used that had similar icons and functions as an AWACS simulator. Despite this, there were sufficient differences in the look-and-feel of this simulator compared to what they use on a day-to-day basis. These differences resulted in a steeper learning curve than anticipated. Additionally, only two hours was allotted for each subject trial and this may not have been enough for all subjects to overcome the learning curve.

The second experiment used Air Force officers from a variety of career fields, most of which did not directly support command and control operations. This, along with the unfamiliarity of the command and control simulator as mentioned earlier, may have resulted in a steeper learning curve than was found in the first experiment. While the second experiment was modified to account for this learning curve by simplifying the tasks, the same limitation on trial times was encountered. Therefore, it is likely that some of the subjects from the second experiment may also not have had enough time to overcome the learning curve. Finally, a limitation found in both experiments may have been the sterile and unrealistic laboratory setting. While every effort was made to get the subjects to adopt the role of a command and control commander, the laboratory setting may have detracted from this objective and resulted in less effective manipulations.

Implications

The results of this research contain important implications for Air Force command and control operations, particularly given the increasing threat of information warfare attacks. One important area in which this research may be useful is training. The findings that a person's pre-disposition to trust computers, both in general situations and specific situations, may prove useful in developing a training program to teach people to be more skeptical of information systems and improve error detection rates. For example, it may prove useful to develop a training method that reduces a person's trust both in computer in general and in C2 environments. By doing so, it may cause decision-makers to be more conservative and verify information prior to making a decision.

However according to the OODA Loop theory, in doing so it may also increase the decision-making duration and therefore prove to be more of a liability.

Another area where this research may provide useful is in developing information warfare tactics. For instance, a psychological warfare tactic could be designed to manipulate the enemy's trust in their information system safeguards. While the findings of this research showed limited evidence that external safeguards affect trusting behavior, there was some evidence to suggest that lowering a decision-makers trust in an external safeguard would decrease trust and may, therefore, increase their decision-making time.

Finally, the findings from this research may prove useful for helping to determine a more effective organizational structure in command and control units like the Combined Air Operations Center (CAOC). The CAOC functions with a similar collect mind concept as observed by Weick and Roberts (1993). This implies that each person in the CAOC has an aggregate mental picture of the effectiveness of computer security measures. Therefore, understanding how trust in an external safeguard may prove useful in determining how to organize and operate this type of command and control unit.

Recommendations for Future Research

The findings from this study are encouraging enough to continue this stream of research. While some evidence was found in this study to suggest that an individual's dispositional trust and situational decision to trust explains some of the variance in predicting trusting behavior, it is not clear if these affects hold true in a team environment. Both experiments employed in this research studied individual behaviors, however in real-world command and control environments it is more likely that

individuals are only a part of a command and control team. For instance, an AWACS crew consists of several individuals each serving in a specialized function but interacting with other members of the team. Therefore, it would prove beneficial to the Air Force to understand how an individual's trust in computer systems is affected in a team-based environment. For instance, one interesting research question would be to see if a spoofing event detected by one member of the team spread to other team members.

Another possible are of research would be to examine some of the other constructs of trust offered in McKnight and Chervany's (1999) model of trust. For instance, trusting belief is defined as the trust a person has in a specific person or object. It would be useful to understand how much of a person's trust in computer systems is explained by their trusting belief in a specific computer system.

Finally, as observed in Muir's (1994) and other's research it would interesting to see trust degrades following an intentional computer malfunction in the same way it degrades following an unintentional malfunction. Additionally, it would be beneficial for the Air Force to examine if trust degrades more and over a longer period in following an intentional malfunction versus an unintentional malfunction.

Summary

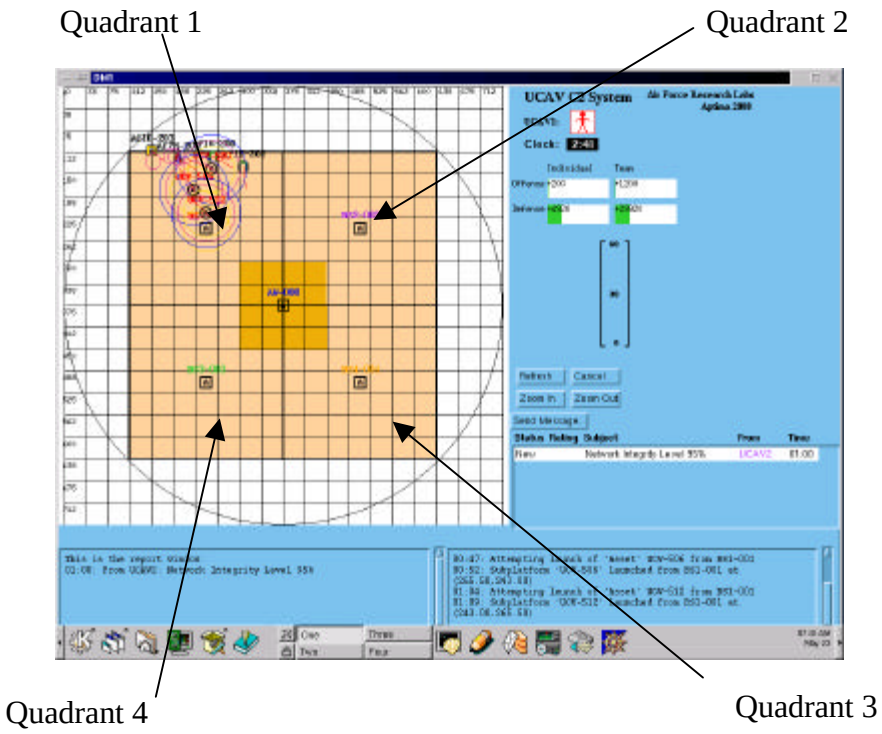
There appears to be strong evidence that attitudes like situational decision to trust effects the trusting behavior of military commander's in C2 environments. Perhaps the most surprising and disturbing result was the failure to prove that information warfare has any effect on persons trusting behavior. These results have important implications for the United States Air Force, especially in the areas of defensive and offensive information

warfare. The findings from this study suggest the need for future research, both in individual behavior and in group behavior. Perhaps one of the most important questions for future research should be to determine if the cost of making people less trustful, and therefore more prone to detecting errors in information systems is worth the speed and accessibility advantage offered by these systems. This accuracy versus speed trade off is suggested in Boyd's (1987) OODA Loop theory.

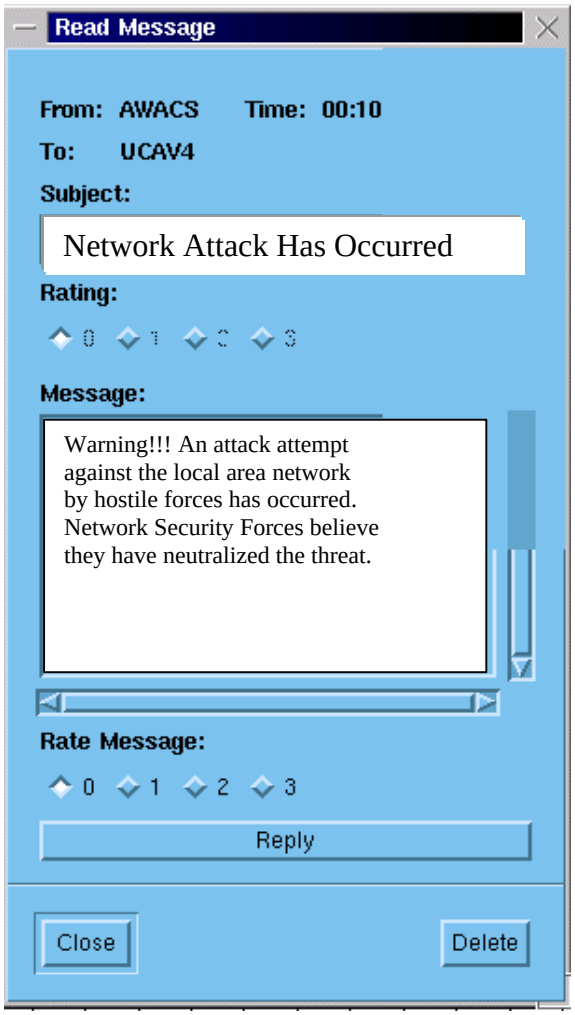
This research indicates that trust in external safeguards may actually have an opposite effect than the one theorized by McKnight and Chervany (1999). Additionally, the findings from these experiments suggest that in a C2 environment, especially a fast-paced, combat environment, the perception of information warfare attacks may not have a significant effect on decision-making behavior. Finally, the results of these experiments offer support for at least one facet of trust offered by McKnight and Chervany (1999), Situational decision to trust. As the Air Force, and in-fact most of society, continues to relay on information systems, future studies are needed to help understand how each of these facets of trust effect decision-making, especially given the going threat of information warfare.

APPENDICIES

Appendix 1: Air Space Boundary Layout



Appendix 2: IW Threat Message



Appendix 3: Scenario Brief

TIME: June 25, 2005

LOCATION: 766th UCAV Ops Squadron, Operating Location Alpha

BACKGROUND:

You are an operations crewmember of the newly formed 766th Unmanned Combat Aerial Vehicle (UCAV) Operations Squadron (766 UOS) deployed in Southwest Asia. The 766 UOS consists of a squadron headquarters located in Dahrain, Saudi Arabia, and five remote operating locations dispersed along the Saudi Arabian border with Iraq. Each operating location consists of an operations cab, communications cab, remote landing field, inflatable hangar, and various tents for sleeping, eating, and other living requirements. Each operating location is responsible for maintaining and controlling 20 of the new UCAVs, commonly referred to as the Viper. Due to the advanced technology and ease-of-use of the UCAV operations system, a single crewmember is capable of controlling up to 3 Vipers and a Tanker aircraft.

THE PRESENT

You have just relieved the night shift after attending the crew changeover briefing where you received the standing mission briefing, Intelligence briefing, and the Rules of Engagement briefing. The following is a summary of the information you received:

MISSION: Defend the airspace around the northern Saudi Arabian city of Jhadamir against any and all unauthorized aircraft. Operating Location Alpha is one of four UCAV operation cabs dispersed around this defended airspace. You are responsible. for air surveillance, track identification, and weapon interdiction for one the upper left quadrant

Appendix 3: Scenario Brief (continued)

INTEL BRIEF: The Iraqis have acquired new computer technology from the Peoples Republic of China's Information Warfare Force (IWF). This technology is thought to include some of the most advanced network attack and information manipulation systems in the world. Sources report Chinese advisors from the IWF have been seen in and around the Iraqi-Saudi Arabian border. The Chinese have recently been successful in demonstrating an Information Warfare tactic known as Strategic Information Manipulation (SIM) against the Taiwanese government. SIM is a technique whereby a computer system is covertly accessed and real-time tactical information is manipulated in order to confuse or spoof the recipient. Intel also reports that satellite imagery has confirmed the Iraqi military's recovery of several air-launched missiles armed with chemical warheads from hidden desert bunkers. These missiles have been distributed to Iraqi air bases just north of the Iraqi No-Fly zone. In early May, Iraqi officials stated on Iraqi national television that the Iraqi government demands the immediate and unconditional withdrawal of all forces in and around the Iraqi No-fly zone. In addition, they stated that if these forces were not withdrawn by the June first then the Iraqi military will use weapons of mass destruction on those forces and the countries that host them. Intel sources and satellite imagery indicate an massive Iraqi air assault is imminent.

RULES OF ENGAGEMENT: By the order of the President of the United States, all US military forces are authorized to fire upon any suspected hostile aircraft. Unknown air tracks should be considered hostile.

Appendix 4: Simulation Scoring System

- Destroy Hostile track = +10 points to Offense Score
- Request Info from AWACS = -5 to Offense Score
- Hostile enters Outer No-fly Zone = -1 points per second to Defense Score
- Hostile enters Inner No-fly Zone = -3 points per second to Defense Score
- Destroy Friendly track = -100 points to Defense Score
- UCAV Destroyed = -25 points to Offense Score

Appendix 5: Multiple Choice Test

Training Evaluation

Please circle the correct answer:

1. For purposes of this evaluation, the UCAV C2 system processes and displays information reliably _____ of the time.
   a. 100%
   b. 75 %
   c. 50 %
   d. 25 %

2. The role of the Network Security Force is to _____
   a. Monitor the network only
   b. Protect the network only
   c. Monitor and Protect the network
   d. None of the above

3. An upside "V" shaped icon that is colored red represents what type of track?
   a. Friendly
   b. Hostile
   c. Unknown
   d. None of the above

4. The information warfare tactic that covertly manipulates data to spoof the operator is called _____
   a. Denial of Service
   b. Information Manipulation
   c. Hacking
   d. None of the above

5. The main components of the UCAV C2 system are _____
   a. The computer system, the ground station, and the UCAVs
   b. The computer system, the Network Security Forces, and the AWACS
   c. The Network Security Forces, the computer system, the ground station, and UCAVs
   d. None of the above

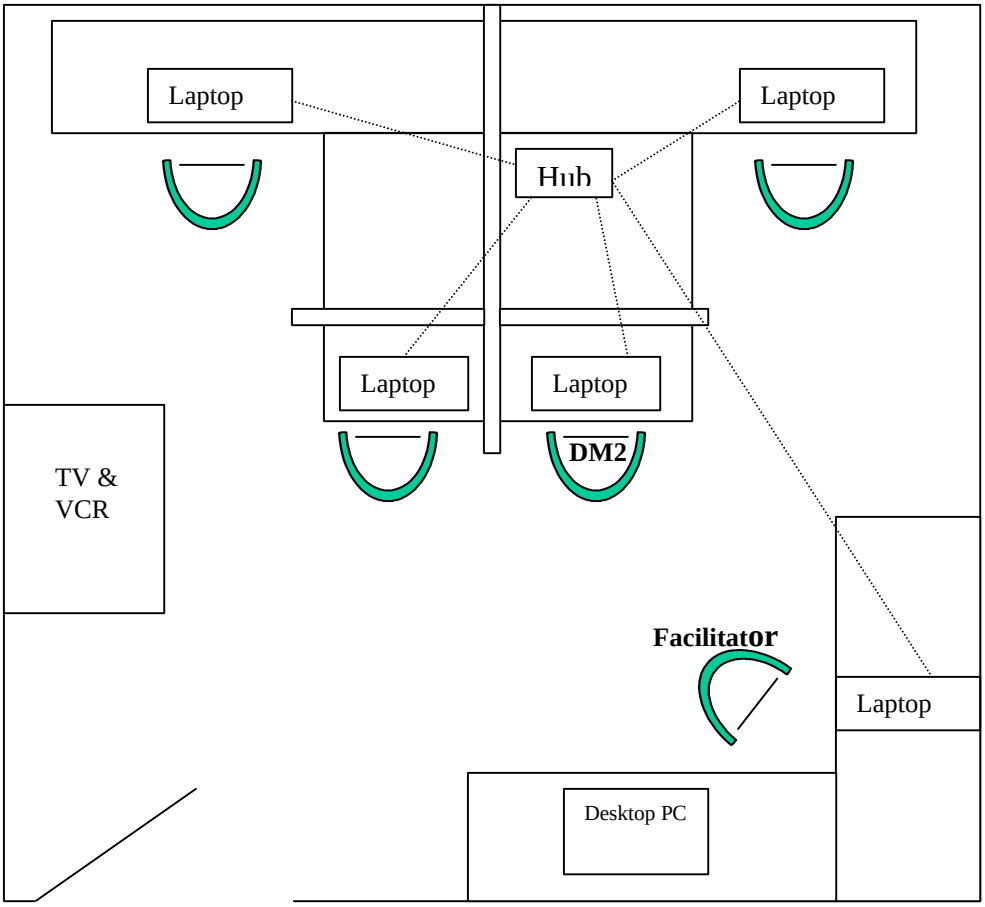
Appendix 5: Multiple Choice Test (continued)

6. A secondary means by which you can verify the track identity is to _____
   a. Send a request to the UCAV pilot
   b. Send a request track info message to the AWACS
   c. Send a free text e-mail message to the Network Security Forces
   d. None of the above
7. The UCAVs will _____
   a. Automatically determine the identity of the track once in sensor range
   b. Detect ground, sea, and air tracks
   c. Only detect the presence of a track and classify it as Unknown
   d. None of the above
8. The outer blue sensor ring represents _____
   a. The weapons range
   b. The UCAV's range
   c. The vulnerability range
   d. The sensor range
9. The inner yellow sensor ring represents _____
   a. The weapons range
   b. The UCAV's range
   c. The vulnerability range
   d. The sensor range

10. The middle red sensor ring represents _____
   a. The weapons range
   b. The UCAV's range
   c. The vulnerability range
   d. The sensor range

11. The Network Security Force (NSF) is _____ effective in protecting and monitoring the network.
   e. 100%
   f. 90 %
   g. 60 %
   h. 25 %

Appendix 6: Experiment Room Layout



Appendix 7: Randomized Block Design

Day	Time	System trust Treatment Group	IW Treatment Group	DM Position	Participant Number
12 Jun 00	0800	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
	1030	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
	1400	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
13 Jun 00	0800	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
	1030	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
	1400	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
14 Jun 00	0800	High	Not Present	1	
		High	Present	2	
		High	Not Present	3	
		High	Present	4	
	1030	Low	Present	1	
		Low	Not Present	2	
		Low	Present	3	
		Low	Not Present	4	
	1400	High	Not Present	1	
		High	Present	2	
		High	Not Present	3	
		High	Present	4	

Appendix 7: Randomized Block Design (continued)

Day	Time	System trust Treatment Group	IW Treatment Group	DM Position	Participant Number
15 Jun 00	0800	Low	Present	1	37
		Low	Not Present	2	38
		Low	Present	3	39
		Low	Not Present	4	40
	1030	High	Not Present	1	41
		High	Present	2	42
		High	Not Present	3	43
		High	Present	4	44
	1400	Low	Present	1	45
		Low	Not Present	2	46
		Low	Present	3	47
		Low	Not Present	4	48
16 Jun 00	0800	High	Present	1	49
		High	Not Present	2	50
		High	Present	3	51
		High	Not Present	4	52
	1030	Low	Not Present	1	53
		Low	Present	2	54
		Low	Not Present	3	55
		Low	Present	4	56

Appendix 8: Subject Consent Form

Informed Consent Form

Study Overview

Welcome to the experiment. The following is a general description of the study and a reminder of your rights as a potential subject. As in any study, your participation is completely voluntary. If now, or at any point during the study, you decide that you do not want to continue participating, please let the experimenter know and you will be dismissed without penalty. Also, please remember that your name will not be associated with any of the information that you provide during the study. All of the information you provide is absolutely anonymous and confidential.

In this study, you will be working as part of a group to complete two group tasks. You will also be asked to complete two questionnaires during the study. You will first be given a questionnaire to complete, then you will complete the first task as a group, after a short break you will be given the second task to complete as a group, and finally, you will be given a second questionnaire to complete. The experimenter will give you more specific instructions later in the study. If you have any questions or concerns at this time, please inform the experimenter.

For further information

The Air Force Institute of Technology faculty members responsible for conducting this research are Maj. Michael Morris and Maj. Paul Thurston. They would be happy to address any of your questions or concerns regarding this study. Maj. Morris can be reached at 255-3636 ext 4578 and Maj. Thurston can be reached at 255-6565 ext 4315.

If you would like to participate in this study, please sign in the space provided. Your signature indicates that you are aware of each of the following: 1) the general procedure to be used in this study, 2) your right to discontinue participation at any time, and 3) you and your name will not be associated with any of the information you provide.

Printed Name: _____

Signature:_____

Date:_____

Appendix 9: Biometric Data Form

Subject Biographical Profile

Subject ID # _____ Group: _____ Date: _____

Age: _____ Male Female

WD experience (approximate): Years: _____ Months: _____

Occupation: WD AWO SD

Flight Status: Mission Ready or DNIF Current Medications: _____

Total E-3 Flight Hours: _____ Other: (AC type # hrs) _____

Indicate the number of times you participated in the following exercises:

___ Red Flag
___ Green Flag
___ Maple Flag
___ Tactical Fighter Wing ORI
___ NORAD Exercise
___ Coronet Sentry
___ Warrior Flag

Other: _____

Approximate flight hours as CAP _____

Approximate flight hours as STK _____

Approximate flight hours as HVAA _____

Total Number SIM hours (est): _____ Total number EVALS: ____ Last EVAL: _____

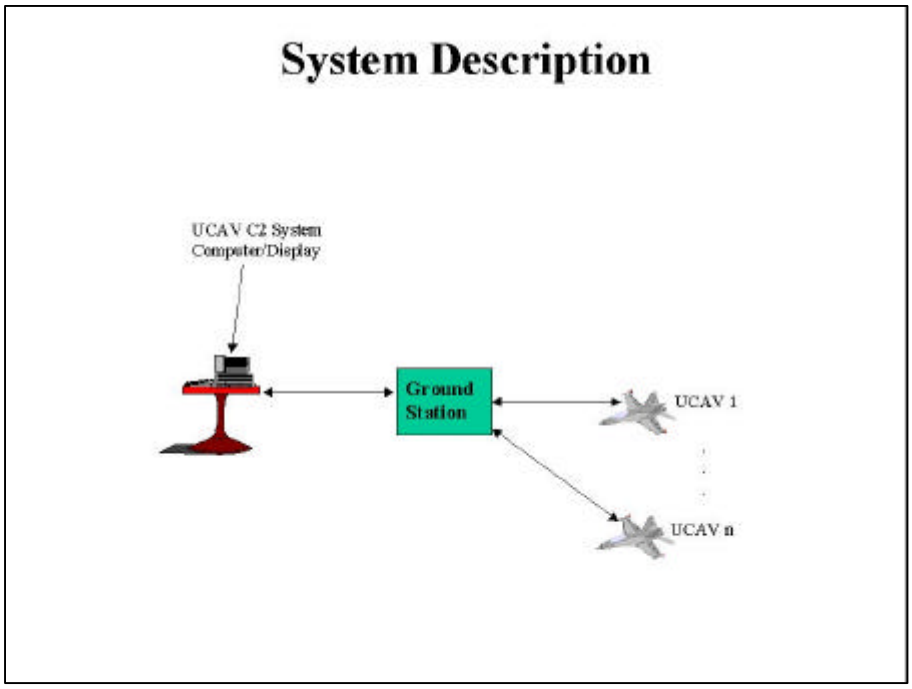
Qualifications Levels: CMR/E CMR/I BMC Instructor

Please indicate how many of the following you have completed in the last 4 months:

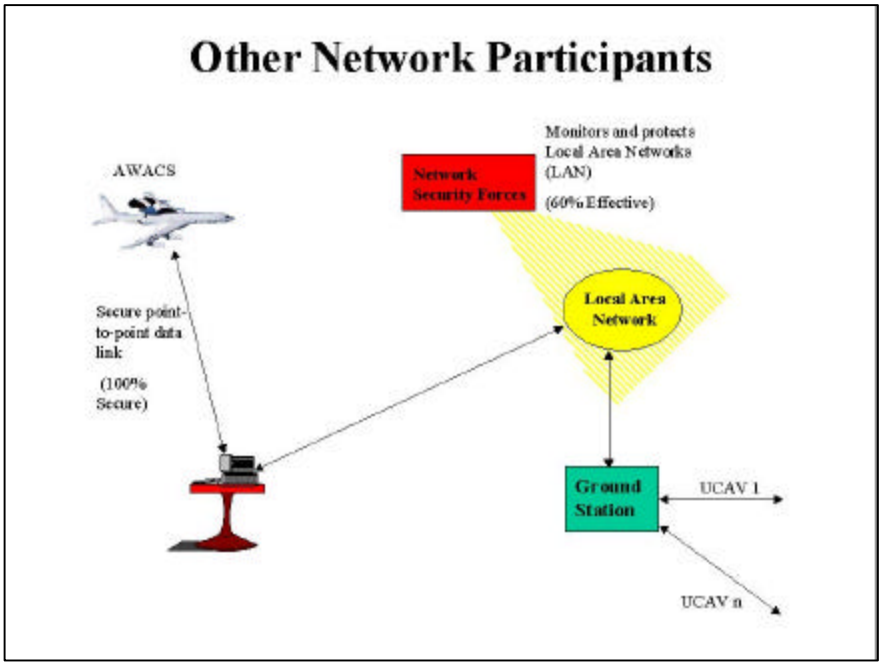
ATD (SIM)	Flight
___ Mission scenarios	___ Weapons Sorties
___ LFE missions	___ 2 v X
___ Close control intercept missions	___ 4 v X
___ 2 v X	
___ 4 v X	
___ Air refueling	
___ EA / EP	

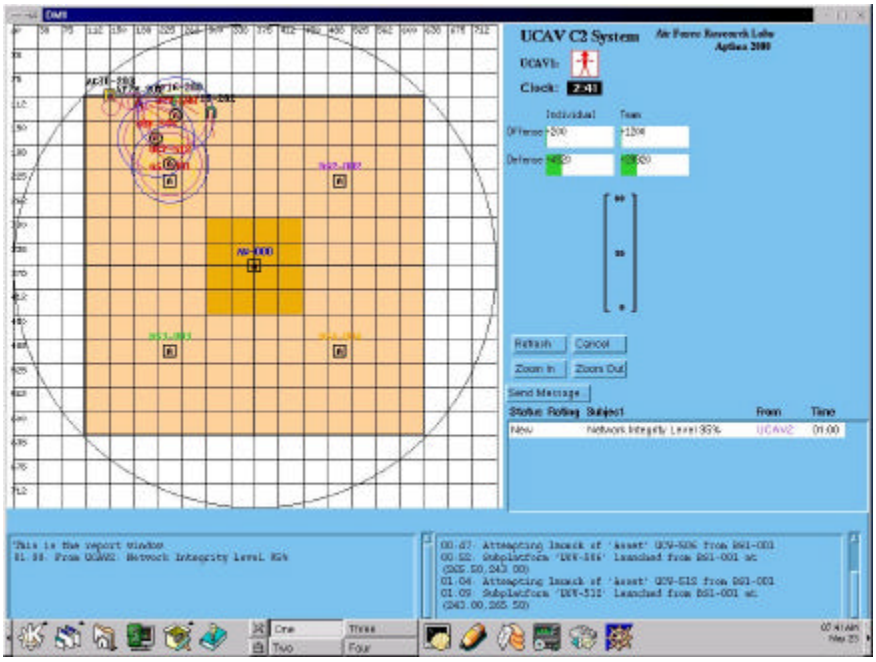
Comments:

Appendix 10: Training Presentation

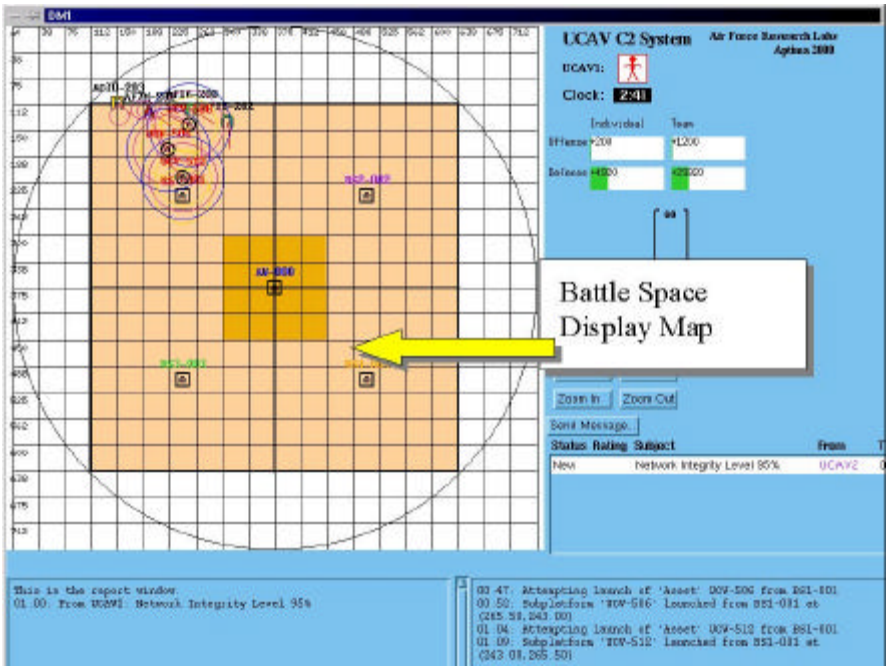


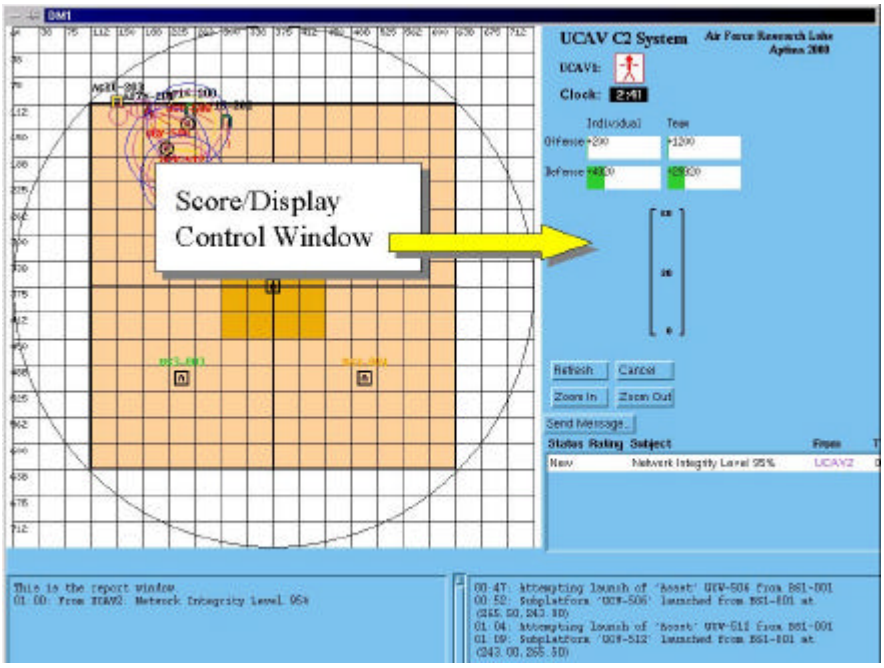
Appendix 10: Training Presentation (continued)



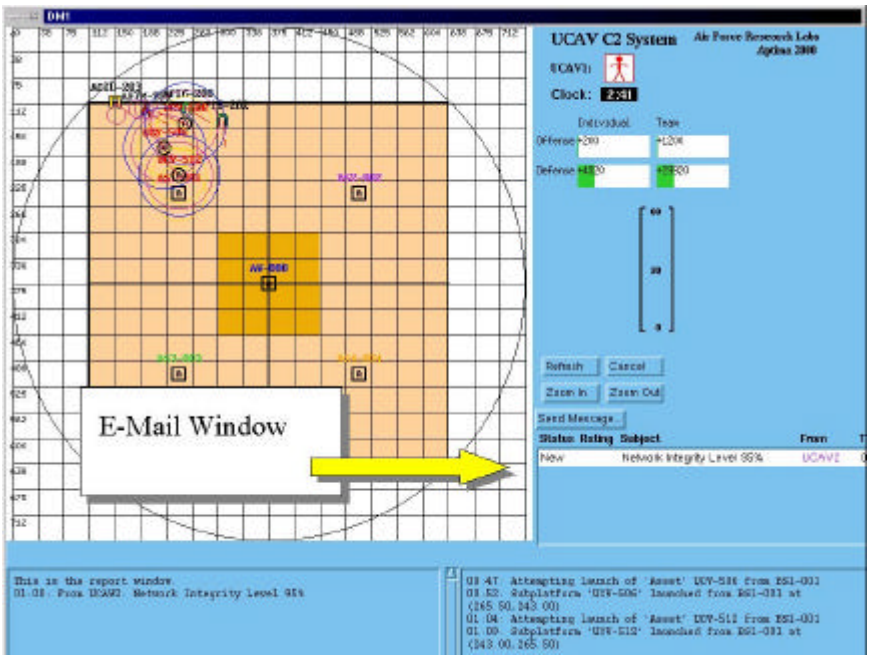


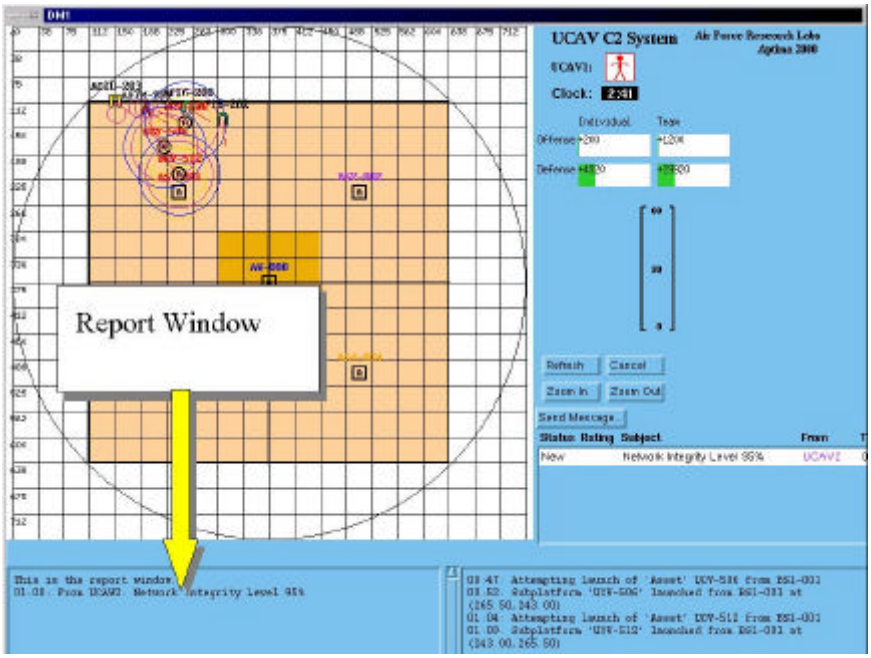
Appendix 10: Training Presentation (continued)



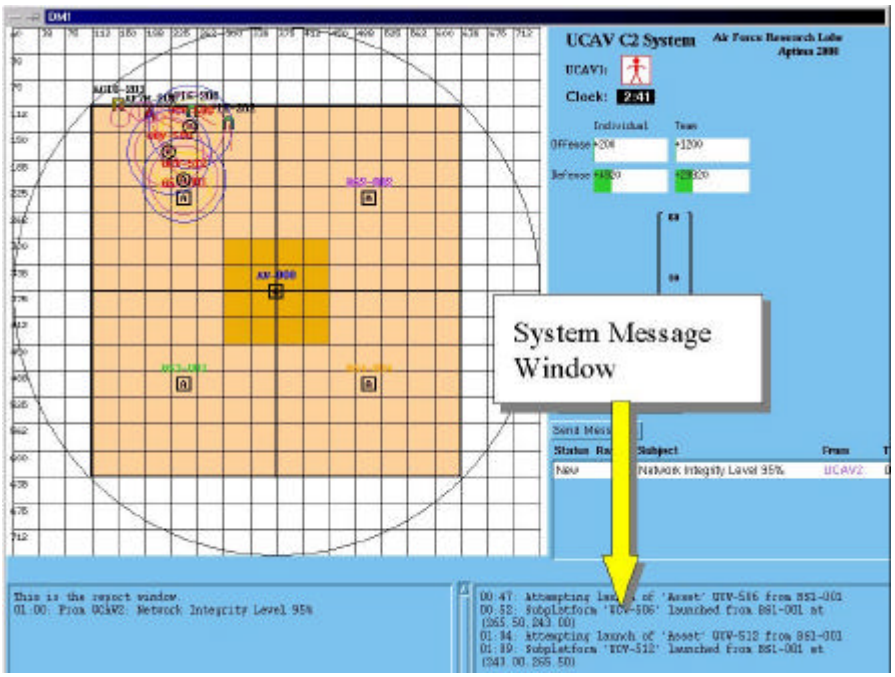


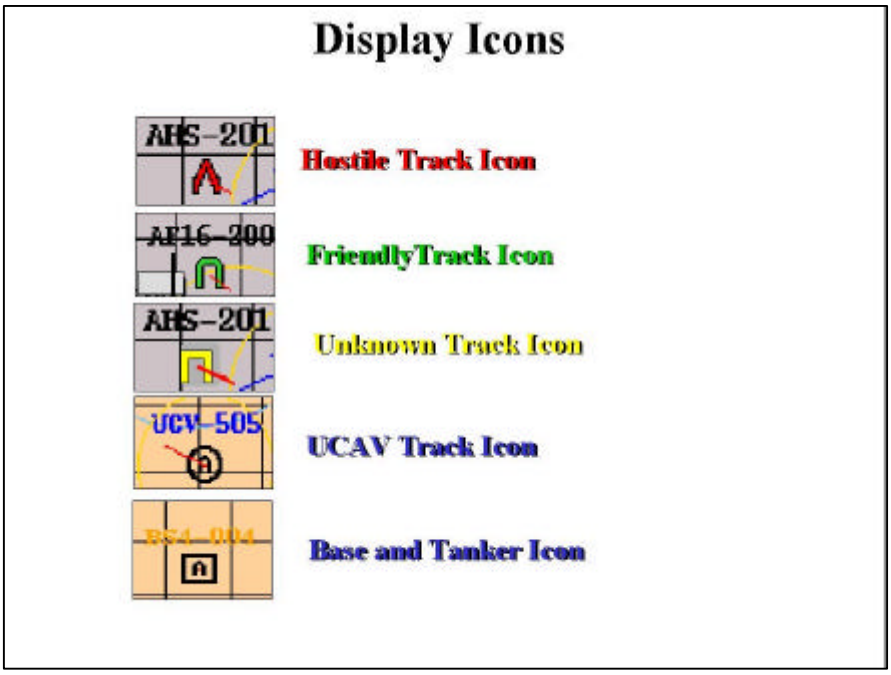
Appendix 10: Training Presentation (continued)



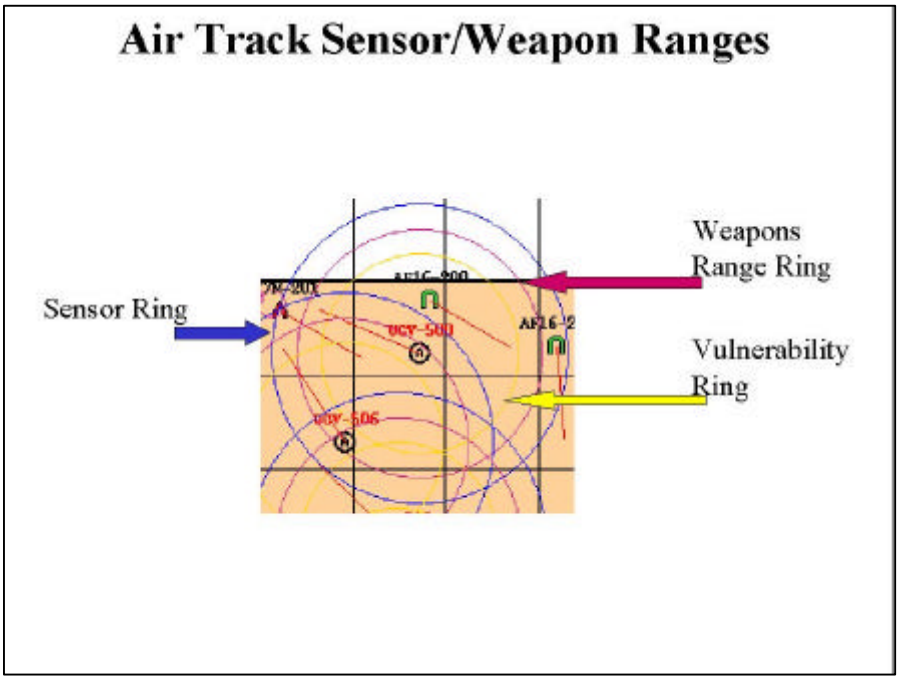


Appendix 10: Training Presentation (continued)





Appendix 10: Training Presentation (continued)



Appendix 10: Training Presentation (continued)

Score System

- Score System:
  - Destroy Hostile track = +10 points to Offense Score
  - Request Info from AWACS = -5 to Offense Score
  - Hostile enters Outer No-fly Zone = -1 points per second to Defense Score
  - Hostile enters Inner No-fly Zone = -3 points per second to Defense Score
  - Destroy Friendly track = -100 points to Defense Score
  - UCAV Destroyed = -25 points to Offense Score

Appendix 11: Pre-Test Survey

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = No Opinion; 4 = Agree; 5 = Strongly Agree

1. ____ If you initiate a task for the average computer system to perform, the computer system will finish it successfully.

2. ____ My typical approach is to trust new computer systems until they prove I shouldn't trust them.

3. ____ I feel assured that the Network Security Forces adequately protects me from attacks to the local area network.

4. ____ Most computer systems are adequate to perform operational-type functions.

5. ____The local area network has enough safeguards to make me feel comfortable using information that is received through it to perform real-world missions.

6. ____ I can always rely on computer systems in an operational setting.

7. ____ When I'm in an operational environment, I feel I can rely on the computer systems I work with in that setting.

8. ____ I usually trust computer systems until they give me a reason not to trust them.

9. ____ There are a good number of computer systems that do not perform as you would expect.

10. ____ I feel confident that the Network Security Force monitoring and protection measures on the local area network make it safe for me to perform real-world missions.

11. ____ In an operational setting, I can depend on computer systems I work with.

Appendix 11: Pre-Test Survey (continued)

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = No Opinion; 4 = Agree; 5 = Strongly Agree

11. ____ In an operational setting, I can depend on computer systems I work with.

12. ____ Most computer systems do a haphazard job at what they do.

13. ____ I think I can adequately rely on the computer systems as a tool in an operational setting.

14. ____ Many computer systems are not really adequate to process real-world operational data.

15. ____ I feel I can depend on computer systems in an operational context.

16. ____ I believe that most computer systems do a very good job in what they were programmed to do.

17. ____ I generally give computer systems the benefit of the doubt when I first use them.

18. ____ In general, the local area network is a robust and safe environment in which perform real-world operational missions.

Appendix 12: Post-Test Survey

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = No Opinion; 4 = Agree; 5 = Strongly Agree

18. ____ If you initiate a task for the average computer system to perform, the computer system will finish it successfully.

19. ____ My typical approach is to trust new computer systems until they prove I shouldn't trust them.

20. ____ I feel assured that the Network Security Forces adequately protects me from attacks to the local area network.

21. ____ Most computer systems are adequate to perform operational-type functions.

22. ____The local area network has enough safeguards to make me feel comfortable using information that is received through it to perform real-world missions.

23. ____ I can always rely on computer systems in an operational setting.

24. ____ When I'm in an operational environment, I feel I can rely on the computer systems I work with in that setting.

25. ____ I usually trust computer systems until they give me a reason not to trust them.

26. ____ There are a good number of computer systems that do not perform as you would expect.

27. ____ I feel confident that the Network Security Force monitoring and protection measures on the local area network make it safe for me to perform real-world missions.

28. ____ In an operational setting, I can depend on computer systems I work with.

Appendix 12: Post-Test Survey (Continued)

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = No Opinion; 4 = Agree; 5 = Strongly Agree

11. ____ In an operational setting, I can depend on computer systems I work with.

12. ____ Most computer systems do a haphazard job at what they do.

13. ____ I think I can adequately rely on the computer systems as a tool in an operational setting.

14. ____ Many computer systems are not really adequate to process real-world operational data.

15. ____ I feel I can depend on computer systems in an operational context.

16. ____ I believe that most computer systems do a very good job in what they were programmed to do.

17. ____ I generally give computer systems the benefit of the doubt when I first use them.

18. ____ In general, the local area network is a robust and safe environment in which perform real-world operational missions.

Appendix 12: Post-Test Survey (Continued)

Please answer the following questions:

1 – Not at all; 2 – barely; 3 – No Opinion; 4-Somewhat; 5-Very

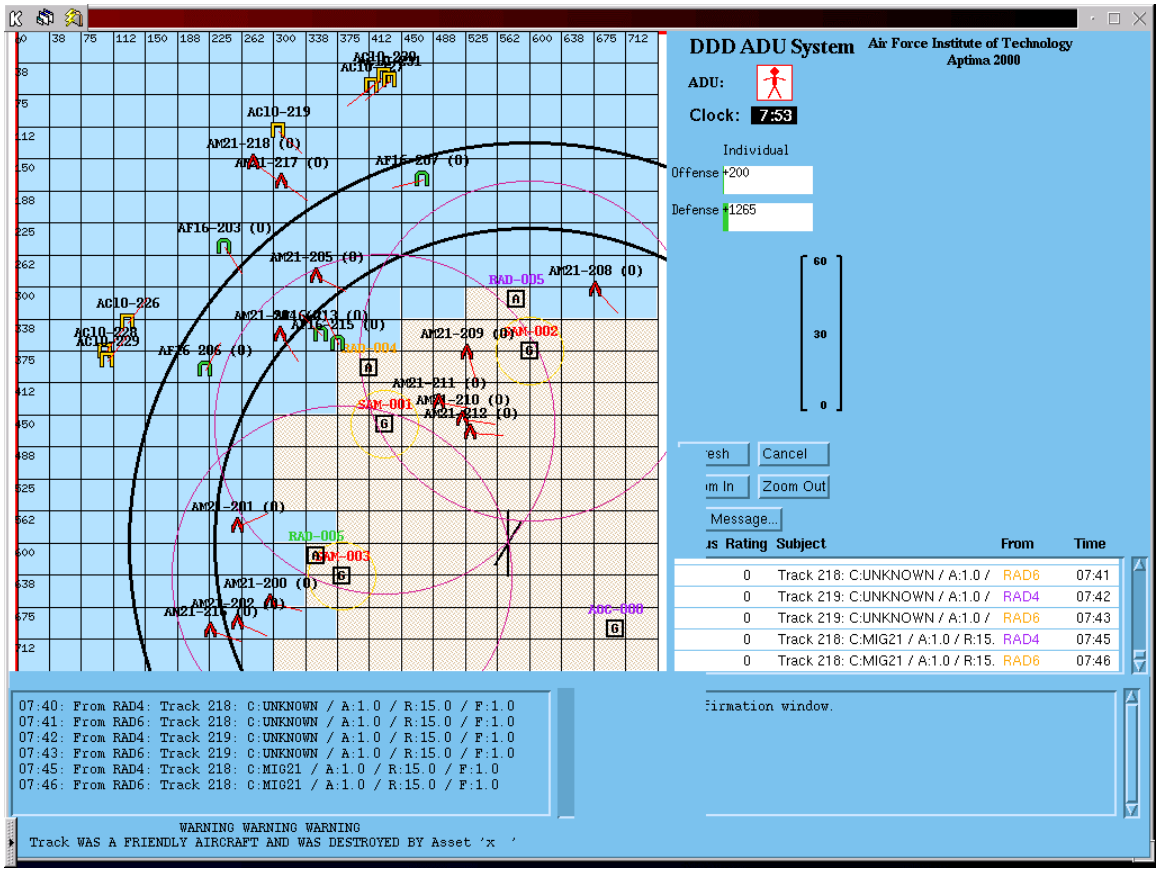
1. ___ In your own opinion, how effective do you feel a system like the UCAV will be for air-to-air missions?

2. ___ In your own opinion, how effective do you feel a unit like the Network Security Force is in monitoring and protecting a local area network against information warfare threats?

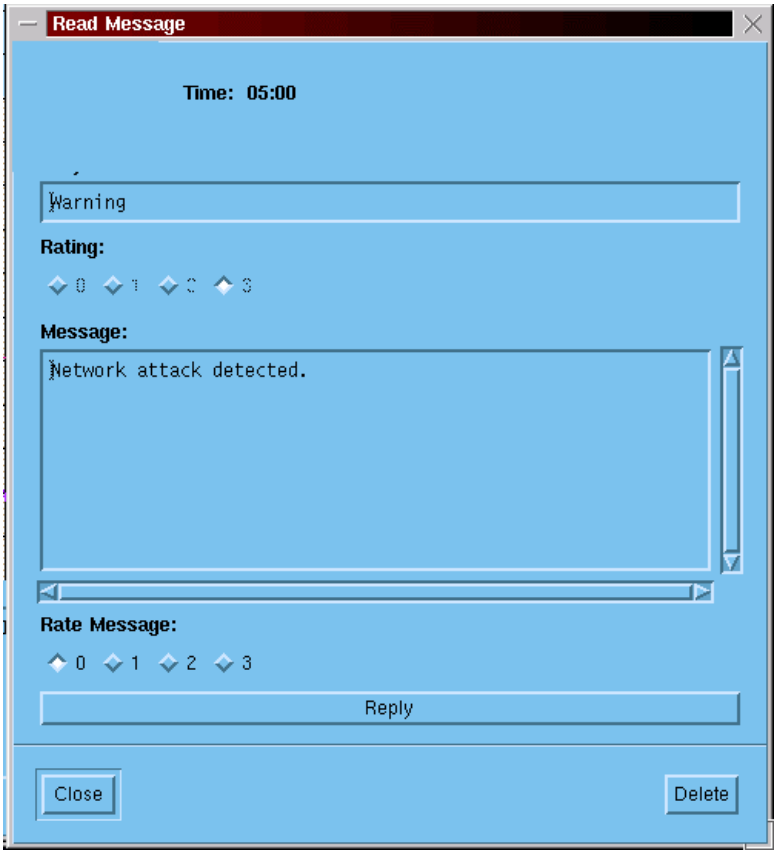
3. ___ In your own opinion, how vulnerable to you feel the Air Force is against information warfare threats?

Please feel free to add any of your own comments:

Appendix 13: Air Space Boundary



Appendix 14: IW Threat Message



Appendix 15: Scenario Brief

BACKGROUND:

You are the air defense commander for 766th Air Defense Unit deployed in Northwest Taiwan. The 766th is a joint air defense unit that integrates tactical ground radar units and surface-to-air missile defense units into a single weapon system. The ADU is a deployed arm of the Air Operation Center and has data connectivity with the AOC, remote radar sites, and remote SAM sites.

THE PRESENT: You have just received the crew changeover briefing where you received the standard mission briefing, Intelligence briefing, and the Rules of Engagement briefing. The following is a summary of the information you received:

MISSION: Defend the assigned air space against any suspected hostile aircraft. The 766th is one of several air defense units dispersed along the coast of Taiwan. You are responsible for air surveillance, track identification, and weapon interdiction. The commander of the 766th is also responsible for assigning a confidence level to all track information and forwarding that information to the Air Operation Center.

Appendix 15: Scenario Brief (continued)

INTEL BRIEF:

In early July, the Chinese government declared it does not recognize the independence of Taiwan, as declared by the Taiwanese government this past June.

In response to this declaration, Taiwan requested and received military support from the United States. This support consisted of two naval battle groups, the regional deployment of 120 fighter and support aircraft, and the local deployment of 5 new Air Defense Units with remotely operated radar and SAM sites.

The deployment was completed in late August. Following this deployment, China threaten that if allied forces were not withdrawn by the first of September then China would reserve the option for a military response. Intel sources and satellite imagery indicate a massive Chinese air assault is imminent.

Intel also reports that the Peoples Republic of China's Information Warfare Force (IWF) have been probing the U.S. forces Wide Area Network. The IWF technology is thought to include some of the most advanced network attack and information manipulation systems in the world. The Chinese have recently demonstrated a successful Information Warfare attack, known as Strategic Information Manipulation (SIM), against the Taiwanese government. SIM is a technique whereby the network is covertly accessed and real-time tactical or strategic information is manipulated in order to confuse or spoof the enemy

RULES OF ENGAGEMENT: By the order of the President of the United States, all US military forces are authorized to use deadly force to interdict hostile aircraft from entering Taiwanese airspace.

Appendix 16: Simulation Scoring System

	Confidence Level					
	0	**1**	**2**	**3**	**4**	**5**
Shoot Enemy	N/A	+20	+40	+70	+110	+160
Shoot Friendly	N/A	-40	-90	-160	-250	-500

If an enemy enters the protected air space, you will **lose 1 point for each second** it remains in the air space.

Appendix 17: Randomized Block Design

Day	Time	System trust Treatment Group	IW Treatment Group	DM Position	Participant Number
12 Jun 00	0800	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
	1030	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
	1400	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
13 Jun 00	0800	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
	1030	High	Present	1	
		High	Not Present	2	
		High	Present	3	
		High	Not Present	4	
	1400	Low	Not Present	1	
		Low	Present	2	
		Low	Not Present	3	
		Low	Present	4	
14 Jun 00	0800	High	Not Present	1	
		High	Present	2	
		High	Not Present	3	
		High	Present	4	28
	1030	Low	Present	1	29
		Low	Not Present	2	30
		Low	Present	3	31
		Low	Not Present	4	32
	1400	High	Not Present	1	33
		High	Present	2	34
		High	Not Present	3	35
		High	Present	4	36

Appendix 17: Randomized Block Design (continued)

Day	Time	System trust Treatment Group	IW Treatment Group	DM Position	Participant Number
15 Jun 00	0800	Low	Present	1	37
		Low	Not Present	2	38
		Low	Present	3	39
		Low	Not Present	4	40
	1030	High	Not Present	1	41
		High	Present	2	42
		High	Not Present	3	43
		High	Present	4	44
	1400	Low	Present	1	45
		Low	Not Present	2	46
		Low	Present	3	47
		Low	Not Present	4	48
16 Jun 00	0800	High	Present	1	49
		High	Not Present	2	50
		High	Present	3	51
		High	Not Present	4	52
	1030	Low	Not Present	1	53
		Low	Present	2	54
		Low	Not Present	3	55
		Low	Present	4	56

Appendix 18: Subject Consent Form

Informed Consent Form

Study Overview

Welcome to the experiment. The following is a general description of the study and a reminder of your rights as a potential subject. As in any study, your participation is completely voluntary. If now, or at any point during the study, you decide that you do not want to continue participating, please let the experimenter know and you will be dismissed without penalty. Also, please remember that your name will not be associated with any of the information that you provide during the study. All of the information you provide is absolutely anonymous and confidential.

In this study, you will be working as part of a group to complete a mission objective. You will also be asked to complete two questionnaires during the study. You will first be given a questionnaire to complete, then following the training, you will be given the second questionnaire to complete. The experimenter will give you more specific instructions later in the study. If you have any questions or concerns at this time, please inform the experimenter.

For further information

The Air Force Institute of Technology faculty members responsible for conducting this research are Maj. David Biros. He would be happy to address any of your questions or concerns regarding this study. Maj. Biros can be reached at 255-3636 ext 4578.

If you would like to participate in this study, please sign in the space provided. Your signature indicates that you are aware of each of the following: 1) the general procedure to be used in this study, 2) your right to discontinue participation at any time, and 3) you and your name will not be associated with any of the information you provide.

Printed Name: _____

Signature:_____ **Date:**_____

Appendix 19: Biometric Data Form

Participant Information Sheet **Participant # _____**

INSTRUCTIONS

This is a short two-part survey to determine the demographic information of the participants in this research as well as their experience level with computer systems. The data collected will be used to aid in the evaluation of the results of the simulation. All information provided will be kept confidential and will not be able to be traced back to the participant.

SECTION 1 – Demographic Information

1. Age _____

2. Rank _____

3. AFSC _____

4. Number of years served in current AFSC _____

5. Total number of years served in the military _____

SECTION II – Computer Experience

1. Are you currently, or have you ever, worked in a computer communications position?

_____

2. Do you consider yourself to be knowledgeable about computers?

3. Are you familiar with how a computer network operates?

4. Are you fluent in any programming languages?

5. Which programs do you use on a frequent basis (circle all that apply)

E-mail	MS Powerpoint
MS Word	UNIX
MS Excel	

Appendix 20: Survey One (Dispositional Trust)

Survey 1 **Participant #:_____**

INSTRUCTIONS

The information you provide will be kept confidential. In addition, your identity will not be linked to this data. The information collected from this form will be used to help evaluate the ADU system and training program.

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = Somewhat Disagree; 4 = No opinion

5 = Somewhat Agree; 6 = Agree; 7 = Strongly Agree

1. _____ If you initiate a task for the average computer system to perform, the computer system will finish it correctly.
2. _____ I believe that most computer systems are consistent.
3. _____ Most computer systems are reliable.
4. _____ I believe that most computer systems are technically competent.
5. _____ I feel I can depend on most computer systems.
6. _____ I can trust most computer systems.

Appendix 21: Survey Two (Situational Decision to Trust)

Survey 2 **Participant #:_____**

INSTRUCTIONS

The information you provide will be kept confidential. In addition, your identity will not be linked to this data. The information collected from this form will be used to help evaluate the ADU system and training program.

Definition: ***Command and Control (C2)***

Command and control (C2) describes the basic job of the military battle commander. The battle commander is responsible for directing military forces to accomplish military objectives against an adversary. In your case, this is air space defense using surface-to-air missiles. C2 objectives often result in material damage and/or human casualties to both the adversary and friendly forces.

Participant Questionnaire

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = Somewhat Disagree; 4 = No Opinion; 5 = Somewhat Agree; 6 = Agree; 7 =Strongly Agree

1. _____In a command and control environment like described in the scenario brief, I believe computers can be relied upon to help commanders make operational decisions.

2. _____ I feel I can depend on computer systems to provide timely and accurate information to battle commanders in a combat situation.

3. _____ In a command and control setting like the one described in the scenario, I feel that I can adequately trust information received from most computer systems.

4. _____ I believe that most computer systems used in deployable battle cabs are secure enough to trust in combat situations.

5. _____ I feel most computer systems used in command and control units are dependable.

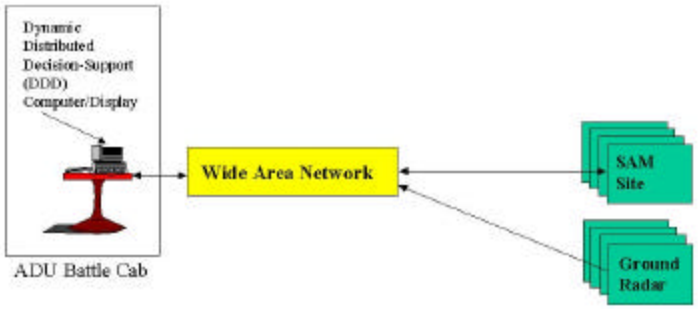
Appendix 22: Training Presentation

Air Defense Unit (ADU)

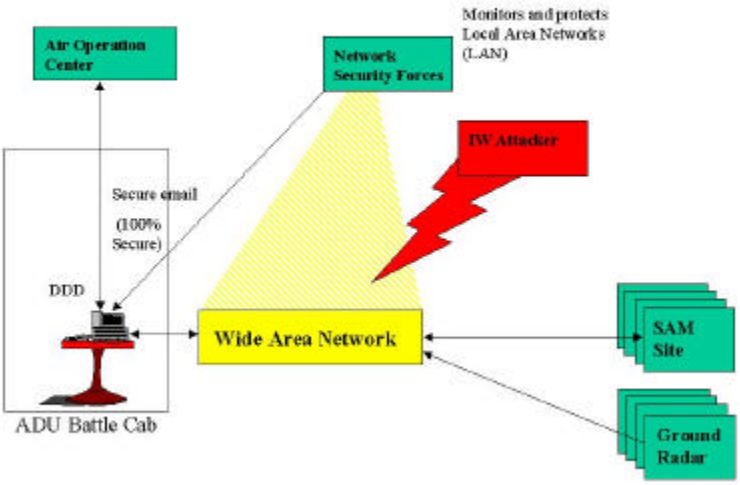
Dynamic Distributed Decision-Support (DDD) System

Field Evaluation

ADU System Description



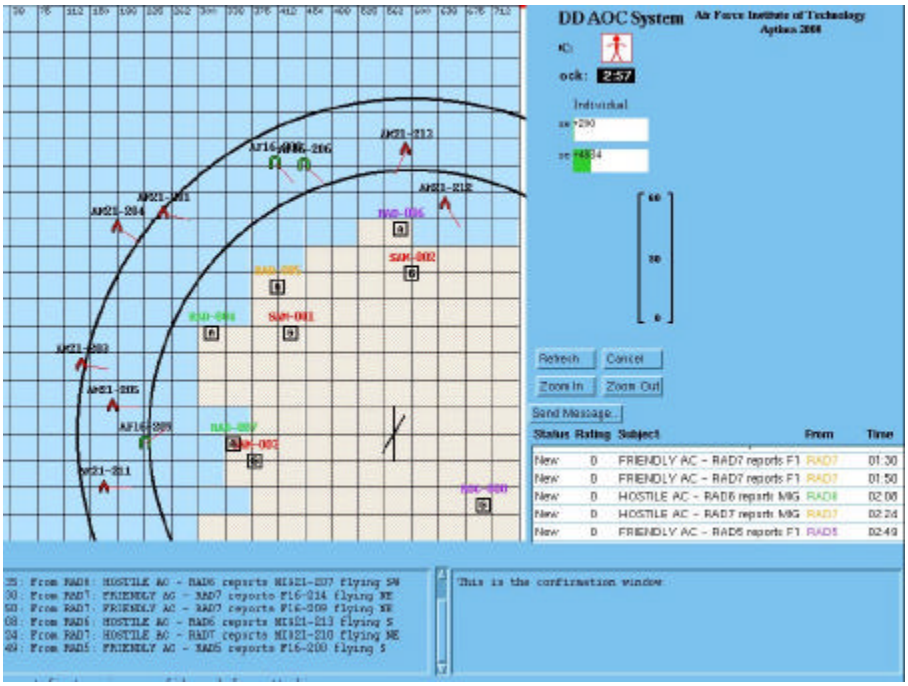
Other Network Participants

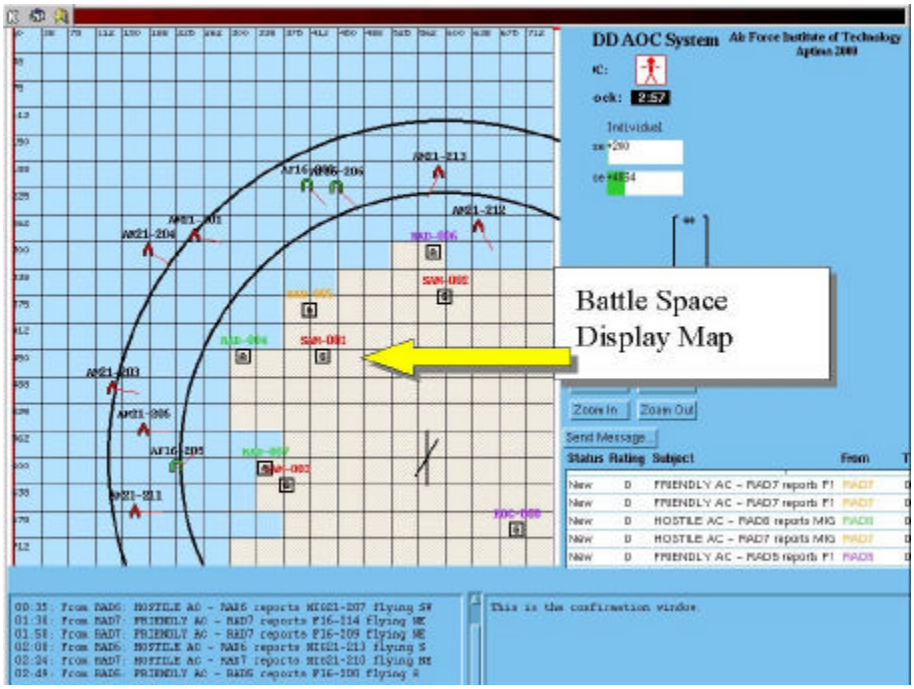


ADU Commander Tasks

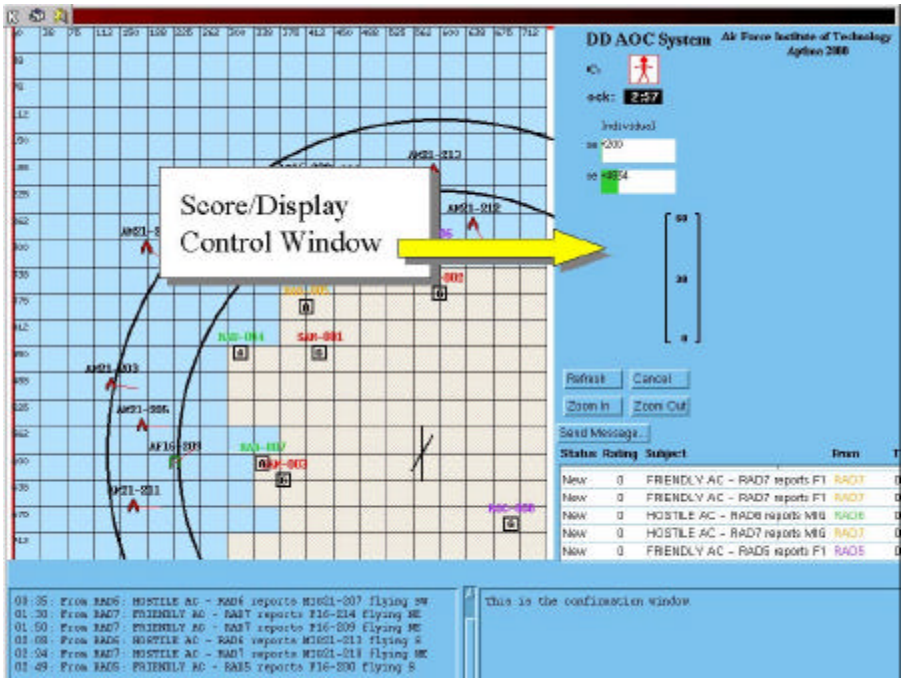
- Monitor Air Space
- Determine Identity of Air Tracks
  - DDD Graphical Display
  - Raw Messages from Sensor Sites
- Assign a Confidence Level to the Track
- Either allow access to protected air space or attack using a Surface to Air Missile

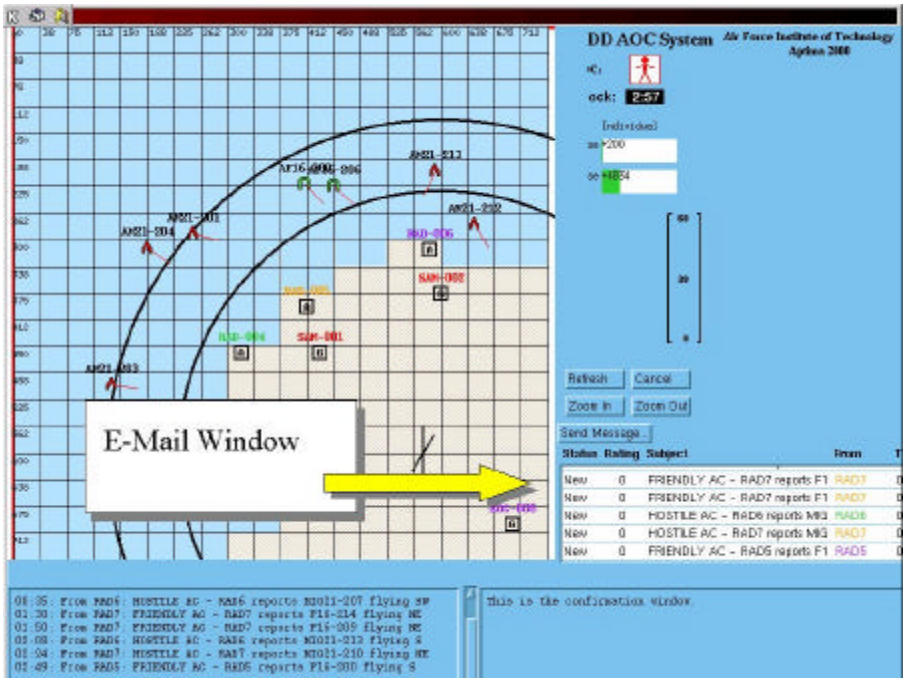
Appendix 22: Training Presentation (Continued)



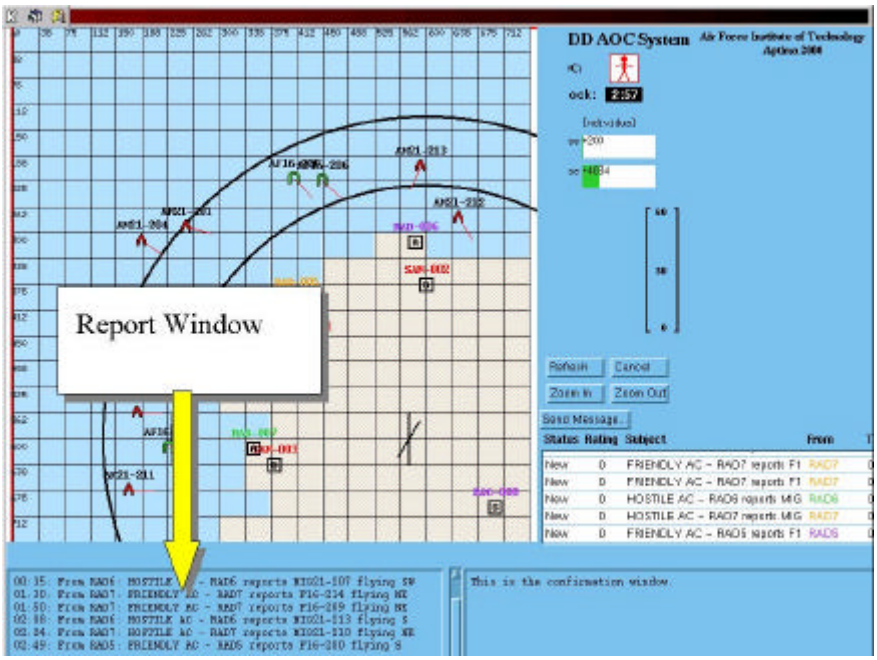


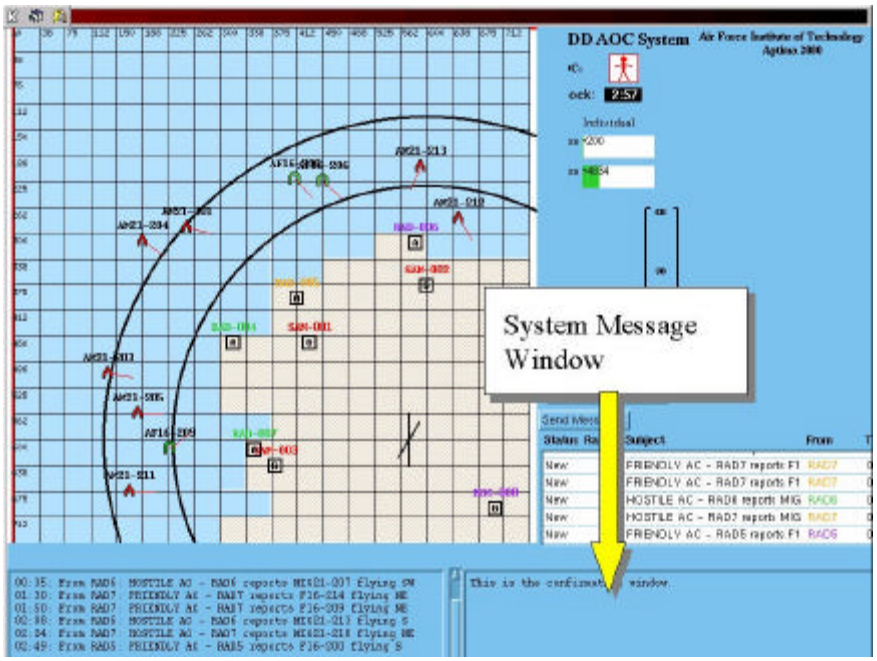
Appendix 22: Training Presentation (Continued)





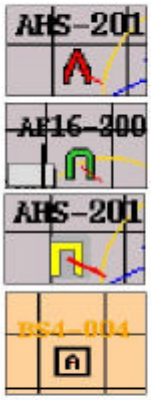
Appendix 22: Training Presentation (Continued)





Appendix 22: Training Presentation (Continued)

Display Icons



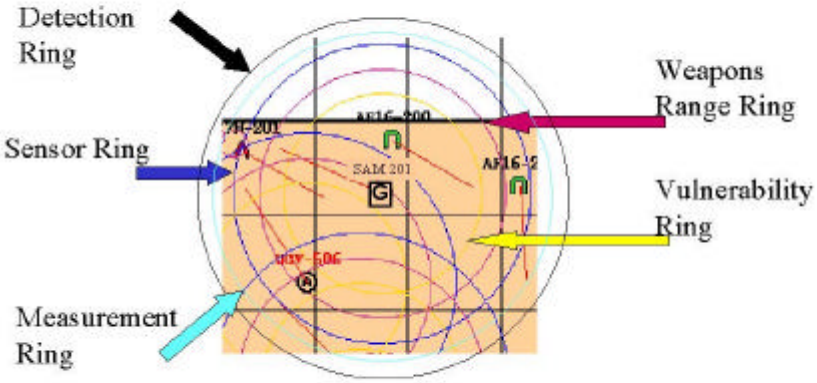
Hostile Track Icon

Friendly Track Icon

Unknown Track Icon

Asset Icon

Air Track Sensor/Weapon Ranges



Appendix 22: Training Presentation (Continued)

Score System

	Confidence Level					
	0	1	2	3	4	5
Shoot Enemy	N/A	20	40	70	110	160
Shoot Friendly	N/A	-40	-90	-160	-250	-500

If an enemy enters the protected air space, you will **lose 1 point for each second** it remains in the air space.

Appendix 23: Survey Three (Trusting Belief)

Survey 3 **Participant #:_____**

INSTRUCTIONS

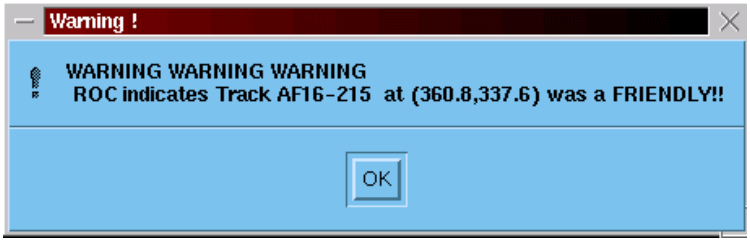
The information you provide will be kept confidential. In addition, your identity will not be linked to this data. The information collected from this form will be used to help evaluate the ADU computer system and training program.

Please answer all of the questions below. Use the scale provided and enter the number that best matches your beliefs.

1 = Strongly Disagree; 2 = Disagree; 3 = Somewhat Disagree; 4 = No Opinion; 5 = Somewhat Agree; 6 = Agree; 7 =Strongly Agree

1. _____ The DDD computer system is predictable.
2. _____ The DDD computer system is consistent.
3. _____ The DDD computer system is technically competent.
4. _____ The DDD computer system has integrity.
5. _____ The DDD computer system is reliable.
6. _____ The DDD computer system is dependable
7. _____ I can trust the DDD computer system.

Appendix 24: Fratricide Warning



Bibliography

Anderson, J. C. & Narus, J. A. 1990. "A model of distributor firm and manufacturer firm working partnerships." Journal of Marketing, 54:42-58.

Anthony, R. N. Planning and control systems: A framework for analysis. Boston, MA: Division of research, Graduate School of Business Administration, Harvard University, 1965

"Automated Armor-Busting Missile Success Keyed to Man-in-the-Loop", National Defense, 527 : 28-29 (April 1997)

Barber, B. The Logic and Limits of Trust. New Brunswick, NJ: Rutgers University Press, 1983.

Birkeland, Paul W., "RLV Regulations – Planning for Evolution", SpaceDaily. www.spacer.com/spacecast/news/oped-99j.html

Biros, David, Still Need Your Full Dissertation Title. Ph.D. dissertation. Florida State University, Somewhere in FL, 1998 (Dissertation Number)

Bisantz, Ann M. "Modeling environmental uncertainty to understand and support dynamic decision-making." Dissertation Abstracts International: Section B: The Sciences & Engineering, (59(3-B), 1301 (September, 1998).

Bisantz, Ann M., James Llinas, Younho Seong, Richard Finger, and Jiun-Yin Jian. "Empirical Investigations of Trust-related System Vulnerabilities in Aided, Adversarial Decision Making." Report for the Center for Multi-source Information Fusion. Department of Industrial Engineering, State University of New York at Buffalo, Amherst, NY. January, 2000

Borgmann, Albert. Crossing the Postmodern Divide . Chicago: University of Chicago Press, 1992.

Bonoma, T. V.. Conflict, cooperation, and trust in three power systems. Behavioral Science, 21(6): 499-514. (1976)

Boyd, John R. "Organic Design for Command and Control," excerpt from A Discourse on Winning and Losing, a selection of unpublished notes and visual aides, compiled from 1976-1992, 5-12.

Bromiley, P. & Cummings, L. L. "Organizations with trust." in Research in Negotiations: 219-247, 5th edition, (Eds) Bies, R., Lewicki, R., & Sheppard, B., Greenwich, CN: JAI Press, 1995

Cannon-Bowers, Janis A., Eduardo. Salas, and J. Grossman. "Improving tactical decision making under stress: Research directives and applied implications." Conference presentation at the International Applied Military Psychology Symposium, Stockholm, Sweden. 1991.

Cannon-Bowers, Jannis A., Eduardo. Salas, and John S. Pruitt. "Establishing the boundaries of a paradigm for decision-making research," Human Factors, 38(2): 193-205 (1996).

Cassell, Justine and Timothy Bickmore, "External Manifestations of Trustworthiness in the Interface", Communications of the ACM, 43(12): 50-56 (December 2000)

"Cornerstones of Information Warfare," A United States Air Force doctrine proposal for information warfare. http://www.af.mil/lib/corner.html. 11 September, 1999.

Davis, F. D. "A Technology Acceptance Model for Empirically Testing New End-User Information Systems: Theory and Results," Doctoral dissertation, Sloan School of Management, Massachusetts Institute of Technology, 1986.

De Ward, Dick and Karel A. Brookhuis, "Driver Support and Automated Driving Systems: Acceptance and Effects on Behavior," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

DeSanctis, G. and M. S. Poole. "Capturing the Complexity in Advanced Technology Use: Advanced Structuration Theory," Organization Science: A Journal of the Institute of Management Sciences, 5(2): 121 (1994).

Dillon, Andrew and Michael G. Morris. "User Acceptance of Information Technology: Theories and Models" in Annual Review of Information Science and Technology (ARIST), 31: 3-32. Ed. Williams, Martha E. Medford, NJ: Information Today, 1996.

Dobing, B. 1993. Building trust in user-analyst relationships. Unpublished doctoral dissertation, Carlson School of Management, University of Minnesota.

Drillings, Michael and Daniel Serfaty. "Naturalistic decision making in command and control." in Naturalistic Decision Making Ed. Zsambok, Caroline E., Klein, Gary, et al. Mahwah, NJ: Lawrence Erlbaum Associates Inc., 1997.

Entin, Elliot E. and Daniel Serfaty. "Sequential Revision of Belief: An Application to Complex Decision Making Situations," IEEE Transactions on Systems, Man, and Cybernetics – Part A: Systems and Humans, 27(3): 289-301 (May 1997).

Fishbein, M. and I. Ajzen. Belief, attitude, intention and behavior: An introduction t theory and research. Reading, MA: Addison-Wesley, 1975.

Fisk, Arthur D. and Mark W. Scerbo, "Automatic and Control Processing Approach to Interpreting Vigilance performance: A Review of Reevaluation", Human Factors, 19(6): 653-660 (December 1987)

Friedman, Batya, Peter H. Kahn Jr., and Daniel C. Howe, "Trust Online", Communications of the ACM, 43(12): 34-40 (December 2000)

Gabarro, J. J. "The development of trust, influence, and expectations." In Interpersonal behavior: Communication and understanding in relationships: 290-303. (Eds) Athos, A. G. & Gabarro, J. J.,Englewood Cliffs, NJ: Prentice-Hall, 1978

Giffin, K. "The contribution of studies of source credibility to a theory of interpersonal trust in the communication process." Psychological Bulletin, 68(2): 104-120 (1967)

Golembiewski, R. T. and M. McConkie. "The Centrality of Interpersonal Trust in Group Processes." In Theories of Group Processes. Ed. Cooper, G. L. London: John Wiley & Sons, 1975.

Hall, Richard H. Organizations: Structures, Processes, and Outcomes. London: Prentice-Hall, 1996.

Harnett, D. L. & Cummings, L. L. Bargaining behavior: An international study. Houston: Dame Publications, 1980

Jian, Jiun-Yin, Ann M. Bisantz, and Colin G. Drury. "Foundations for an empirically determined scale of trusting automated systems." International Journal of Cognitive Ergonomics, 4(1): 53-71 (2000).

Jorna, P. G. A. M., "Automation and Free(er) Flight: Exploring the Unexpected," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

Kaempf, George L., Gary Klein, Marvin L. Thordsen, and Steve Wolf. "Decision Making in Complex Naval Command-and-Control Environments," Human Factors, 32(2): 220-231 (1996).

Kee, H. W. & Knox, R. E. "Conceptual and methodological considerations in the study of trust and suspicion." Journal of Conflict Resolution, 14:357-366. (1970)

Kellner, Douglas. "New Technologies, TechnoCities, and the Prospects for Democratization." Online course material for UCLA Education, Technology and Society course. www.gseis.ucla.edu/courses/ed253a/newDK/techcity.htm. December 1997.

Kirwan, Christopher. Metaphysics. – Books [Gamma, Delta, and Epsilon], Translation of Aristotle's Metaphysics, (Second Edition). Oxford: London, 1993.

Klein, G. A. "Naturalistic models of C3 decisionmaking."in Science of command and control: Coping with uncertainty Ed. Johnson S. and Levis A. Washington, DC: AFCEA International Press, 1988.

Kuehl, Dan. "Joint Information Warfare: An Information-Age Paradigm for Jointness," Essay on Strategy, http://www.ndu.edu/ndu/irmc/publications/forum105.htm , 20 July 2000.

Lawler, E. E. & Rhode, J. G. Information and control in organizations. Pacific Palisades, CA: Goodyear Publishing Company, 1976

Lee, John and Neville Moray. "Trust, control strategies and allocation of function in human-machine systems," Ergonomics, 35(10): 1243-1270 (1992).

Luhman, N. Trust and Power. Ann Arbor, MI: University Microfilms International, 1991.

Mayer, Daryle (Master Sgt, USAF). "Keeping Air Force secrets secret," AirForce News. http://www.af.mil/news/Jun2000/n20000621_000943.html . 21 June 2000.

Mayer, R. C., J. H. Davis, and F. D. Schoorman. "An integrative model of organizational trust." Academy of Management Review, 20: 709-734 (1995).

McCornack, Steven A., Timothy R. Levine, Kelly Morrison, and Maria Lapinski, "Speaking of Information Manipulation: A Critical Rejoinder," Communication Monographs, 63(1): 83 (1996)

McKnight, D. Harrison and Norman L. Chervany. "The Meanings of Trust." Research working paper, n. pag. http://www.misrc.umn.edu/wpaper/wp96-04.htm. 26 October 1999.

McLuhan, Marshal. The global village : transformations in world life and media in the 21st century . New York: Oxford University Press, 1989

Mosier, Kathleen L., Linda J. Skitka, and M. D. Burdick, "Accountability and Automation Bias," International Journal of Human-Computer Studies, 52(4): 701 (2000)

Mosier, Kathleen L, Linda J. Skitka, and Susan T. Heers, "Automation and Acountability for Performance," Ames Research Center and NASA Human Factors Research and Technology Division, human-factors.arc.nasa.gov/Ihpublications/mosier/OSU95/OSU_Mosier.html. 21 July 2000.

Muir, Bonnie M. "Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems," Ergonomics, 39(3): 1905-1922 (1994)

Muir, Bonnie M. and Neville Moray. "Trust in automation: Part II. Experimental studies of trust and human intervention in a process control simulation," Ergonomics, 37(11): 429-460 (1996)

Muir, Bonnie M. "Trust between humans and machines and the design of decision aides," International Journal of Man-Machine Studies, 27: 527-539 (1987).

Murray, Steven A. and Barrett S. Caldwell. "Operator Alertness and Human-Machine System Performance During Supervisory Control Tasks," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

Murphy, Elizabeth D. and Kent L. Norman. "Beyond Supervisory Control: Human Performance in the Age of Autonomous Machines," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

Nunally, Jum C. and Ira H. Bernstein. Psychometric Theory. New York: McGraw Hill Company, 1994.

Olson, Judith S. and Gary M. Olson, "i2i Trust in E-commerce", Communications of the ACM, 43(12): 41-44 (December 2000)

Orasanu, Judith M. and Terry Connolly. "The Reinvention of Decision Making," in Decision Maing in Action: Models and Methods. Ed. G. Klein, J. Orasanu, R. Calderwood, and C. E. Zsambok. Norwood, NJ: Ablex, 1993.

Parasuraman, Raja. "Human-Computer Monitoring," Human Factors, 29(6): 695-706 (December 1987)

Randel, J. M. and H. L. Pugh. "Differences in expert and novice situation awareness in naturalistic decision making," International Journal of Human-Computer Studies, 45(5): 579-597 (1996).

Rempel, J. K., J. G. Holmes, and M. P. Zanna. "Trust in close relationships," Journal of Personality and Social Psychology, 42: 95-112 (1985).

Resnick, Paul, Richard Zeckhauser, Eric Friedman, and Ko Kuwabara, "Reputation Systems", Communications of the ACM, 43(12): 45-48 (December 2000)

Riker, W. H. "The nature of trust." In Perspectives on Social Power, 63-81. (Ed) Tedeschi, J. T. Chicago: Aldine Publishing Company, 1971

Roman, Gregory A. "The Command or Control Dilemma: When technology and organizational orientation collide." Essay on Strategy XIV, www.ndu.edu/ndu/inss/books/essa/essaccdw.html , 11 September 1999.

Rotter, J. B. "A new scale for the measurement of interpersonal trust." Journal of Personality, 35(4): 651-665. (1967)

Shneiderman, Ben, "Designing Trust into Online Experiences", Communications of the ACM, 43(12): 57-59 (December 2000)

Seong, Younho, James Llinas, Colin G. Drury, and Ann M. Bisantz. "Human Trust in Aided Adversarial Decision-Making Systems," in Automation technology and human performance. Ed. Scerbo, M. W. and Mouloua, M. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

Shapiro, S. P. "The social control of impersonal trust." American Journal of Sociology, 93(3): 623-658 (1987).

Sheridan, T. B. and R. T. Hennessy. Research and Modeling of Supervisory Control Behavior. Washington: National Academy Press, 1984.

Sheridan, William, "The Paradigm Shift of the Information Age." Literature review. www3.sympatico.ca/cypher/effects.htm , 9 July 2000.

Simon, Herbert A. Administrative Behavior. New York: Free Press, 1957

Simon, Herbert A. "Decision Making in Economics", American Economics Review, June 1959.

Sun Tzu 6th cent B.C. The Art of War / by Sun Tzu. (Ed) Clavell, James. New York: Delecorte Press, 1983.

Tiryakian, E. A. "Typologies." in International encyclopedia of the social sciences, 16: 177-186. Ed. Sills, D. L. The Macmillan Company & The Free Press, 1968.

Van Cleave, John. "Critical Factors in Cyberspace," Research paper submitted to the Department of Joint Military Operations, Naval War College, Newport, RI. February, 1997.

Von Neumann, J. & Morgenstern, O., Theory of Games and Economic Behavior , New York: Wiley, 1944.

Weick, Karl E. and Karlene H. Roberts. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," Administrative Science Quarterly, (38): 357-381 (1993).

Whitehead, YuLin. "Information as a Weapon: Reality versus Promises." Essay. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj97/fal97/whitehead.html , 11 September 1999.

Wickens, C. D. "Automation in Air Traffic Control: The Human Performance Issue," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and M. Mouloua. Mahwah, NJ: Lawrence Erlbaum Associates, 1999.

Wiener, E. L. and R. E. Curry. "Flight-deck automation: promises and problems," Ergonomics, (23): 995-1011 (1980).

Wrightsman, L. S." Interpersonal trust and attitudes toward human nature." In Measures of personality and social psychological attitudes: Vol. 1: Measures of social psychological attitudes: 373-412. (Eds) Robinson, J. P., Shaver, P. R., & Wrightsman, L. S. San Diego, CA: Academic Press, 1991

Yeung, Lorrita N. T., Timothy R. Levine, and Kazuo Nishiyama. "Information Manipulation Theory and Perceptions of Deception in Hong Kong." Communications Reports, 12(1): 1-11 (1999).

Zey, Mary. Decision Making: Alternatives to Rational Choice Models. Newbury Park, California: Sage, 1992

Zuboff, Shoshana. In the Age of the Smart Machine: The Future of Work and Power. Oxford: Heinemann Professional, 1988

Zucker, L. G. Production of trust: Institutional sources of economic structure, 1840-1920. In Research in Organizational Behavior, 8:53-111. (Eds) Staw, B. M. & Cummings, L. L. Greenwich, CN: JAI Press, 1986

Vita

Captain Gregory S. Fields was born on [redacted] in Akron, Ohio. He graduated from Cuyahoga Falls High School in Cuyahoga Falls, Ohio in June 1984. He enlisted in the United States Air Force in December 1985 and served six years as an Administrative Technician. His assignments while enlisted included 7401st Munitions Support Squadron, Rimini, Italy, the 486th Tactical Missile Wing, Woensdrecht AB, The Netherlands, the 7276 Supply Squadron, Iraklion AS, Crete, the 3551st Recruiting Squadron, Elwood, IL, and the 3505th Recruiting Group, Chanute AFB, IL.

He entered undergraduate studies at the University of Akron in Akron, Ohio where he graduated with a Bachelor of Science degree in Computer Science in May 1994. He was commissioned through the Detachment 630 AFROTC at the University of Akron.

His first assignment as a Second Lieutenant was at USSTRATCOM, Offutt AFB, NE where he served as a software analyst in the Missile Warning Branch. In June 1997, he was assigned to the 932nd Air Control Squadron, Keflavik NAS, Iceland where he served as Flight Commander in charge of long haul communications and software maintenance. In August 2000, he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation, he will be assigned to the Air Force Communications Agency.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
20-03-2001	Master's Thesis	Aug 1999 - Mar 2001

4. TITLE AND SUBTITLE

THE EFFECT OF EXTERNAL SAFEGUARDS ON HUMAN-INFORMATION SYSTEM TRUST IN AN INFORMATION WARFARE ENVIRONMENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Fields, Gregory S., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

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

Air Fore Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 P Street Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/01M-07

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

AFOSR
Attn: Dr. Robert L. Herklotz
801 N. Randolph St., Room 732
Arlington, VA 22203-1977
(703) 696-6565

AFRL/HEAI
Attn: Dr. Sam G. Schiflett
2504 Gillingham Dr
Bldg 170, Suite 25
BROOKS AFB, TX 78235-5104
Phone: (210) 536-8139

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This research looks at how human trust in an information system is influenced by external safeguards in an Information Warfare (IW) domain. Information systems are relied upon in command and control environments to provide fast and reliable information to the decision-makers. The degree of reliance placed in these systems by the decision-makers suggests a significant level of trust. Understanding this trust relationship and what effects it is the focus of this study. A model is proposed that predicts behavior associated with human trust in information systems. It is hypothesized that a decision-maker's belief in the effectiveness of external safeguards will positively influence a decision-maker's trusting behavior. Likewise, the presence of an Information Warfare attack will have a negative affect a decision-maker's trusting behavior. Two experiments were conducted in which the perceived effectiveness of external safeguards and the information provided by an information system were manipulated in order to test the hypotheses presented in this study. The findings from both experiments suggest that a person's trust computers in specific situations are useful in predicting trusting behavior, external safeguards have a negative effect on trusting behavior, and that Information Warfare attacks have no effect on trusting behavior.

15. SUBJECT TERMS

Trust, Human-Automation Trust, Naturalistic Decision Making, Command and Control, Information Warfare, Automation Bias, Truth Bias, Theory of Reasoned Action

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Major David Biros, ENV
U	U	U	UU	157	19b. TELEPHONE NUMBER (Include area code) (937) 255-3636, ext 4826

Standard Form 298 (Rev. 8/98)