Air Force Institute of Technology

AFIT Scholar

3-2002

Task Load and Automation Use in an Uncertain Environment

Mark A. Daly

Follow this and additional works at: https://scholar.afit.edu/etd

Part of the Other Operations Research, Systems Engineering and Industrial Engineering Commons

TASK LOAD AND AUTOMATION USE IN AN

UNCERTAIN ENVIRONMENT

THESIS

Mark A. Daly, Captain, USAF

AFIT/GAQ/ENV/02M-05

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GAQ/ENV/O2M-05

TASK LOAD AND AUTOMATION USE IN AN

UNCERTAIN ENVIRONMENT

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 Software Systems Management

Mark A. Daly, BS

Captain, USAF

March 2002

TASK LOAD AND AUTOMATION USE IN AN

UNCERTAIN ENVIRONMENT
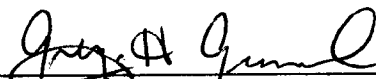
Mark A. Daly, BS
Captain, USAF

Approved:

Lt Col David P. Biros (Chairman)	_31 Jan 02_ date
Dr. Gregg Gunsch (Member)	_31 Jan 02_ date
Lt Col Bradley Ayres (Member)	_31 Jan 02_ date

Table of Contents

List of Figures

List of Tables

Abstract

The purpose of this research was to investigate the effects that user task load level has on the relationship between an individual's trust in and subsequent use of a system's automation. Automation research has demonstrated a positive correlation between an individual's trust in and subsequent use of the automation. Military decision-makers trust and use information system automation to make many tactical judgments and decisions. In situations of information uncertainty (information warfare environments), decision-makers must remain aware of information reliability issues and temperate their use of system automation if necessary. An individual's task load may have an effect on his use of a system's automation in environments of information uncertainty.

It was hypothesized that user task load will have a moderating effect on the positive relationship between system automation trust and use of system automation. Specifically, in situations of information uncertainty (low trust), high task load will have a negative effect on the relationship. To test this hypothesis, an experiment in a simulated command and control micro-world was conducted in which system automation trust and individual task load were manipulated. The findings from the experiment support the positive relationship between automation trust and automation use found in previous research and suggest that task load does have a negative effect on the positive relationship between automation trust and automation use.

TASK LOAD AND AUTOMATION USE IN AN UNCERTAIN ENVIRONMENT

I.   INTRODUCTION

Background

In this information age, automation and information technologies (IT) are woven into every aspect of our lives   We are awakened to start the day by our automatic alarm clocks, and our fresh brewed coffee awaits us as it was pre-programmed to automatically percolate in anticipation of our awakening. We sit down to breakfast and read the freshly printed, personalized, automatically generated, downloaded, and printed paper from our desktop computer. We head to work on an automated subway system that gets us to our destination safely and on time. Throughout the day we are in constant communication with our fellow workers, family members and friends, via our e-mail, cell phones, call forwarding, fax machines, and personal digital assistants, all without giving it a second thought.

Automation and information technologies are not just an aspect of our personnel lives. Over the last decade, the United States has seen a dramatic increase in the use of and reliance upon information technologies and automation for the control and operation of many critical functions. These functions are part of what has become known as our critical information infrastructure. Theses functions include banking and finance, power control, air-traffic control, emergency services, e-commerce, and telecommunications, to name a few. The United States' reliance on such technologies prompted President Clinton, in 1996, to issue an Executive Order establishing a commission on critical infrastructure protection. Its

charge was to study the nation's critical infrastructures and report on their vulnerabilities. The study found increasing dependence on critical infrastructures and increasing vulnerabilities but insufficient awareness of those vulnerabilities (Denning, 1999).

As our world becomes more technologically advanced, society becomes more accustomed to technology and automation as it becomes routine and integral in or lives. We tend to trust the technology, or as Barber (1983) puts it, we gain expectation of technical competence in the technology. The increasing reliance and use in automation and technology has lead researchers to examine the many aspects of human-computer interaction (Parasuraman, 1987; Murray and Caldwell, 1999; Dillion and Morris, 1996; Wickens, 1999). Trust in automation is one area that continues to generate interest among researchers (Sheridan, 1988; Lee and Moray, 1992; Muir 1994; Muir and Moray, 1996; Jian, Bisantz, Drury and Llins, 1998; Tseng and Fogg, 1999; Fields, 2001).

Research has suggested that trust can affect how people accept and rely on automated systems (Sheridan, 1988). For example, researchers have studied issues of human trust in simulated automated environments in which they found that an operator's decision to use automatic or manual control of a processes depended on the trust he had in the system's automation and his confidence in his own abilities to control the system (Muir and Morray, 1996; Lee and Moray, 1994). Others have suggested that people become vulnerable to negative consequences because of their trust in information systems (Bonoma, 1976; Giffin, 1967). These vulnerabilities will only increase as society continues its increasing use of and reliance on information systems and automation.

Research Applicability to the United States Air Force

As with the civilian infrastructure, the Department of Defense (DoD) as well as the individual services are becoming increasingly dependent on automation and information technologies. An example of this reliance on technology was highlighted by Mr. Art Money in 1999, the civilian in charge of the Pentagon's information security, when he stated, " The United States now relies on information systems to such an extent that an attack against those systems would present a genuine threat to U.S. security" (Myers, 1999:1). The change from the more traditional military to a more technologically advanced military has caused what is termed the Revolution in Military Affairs or RMA (Metz, 2000). The RMA is the transforming of the U.S. military into a leaner, faster, higher-tech fighting machine, of which automation is a key component. The U.S. Military is noted for considering advanced technology to be a force multiplier, a force extender, and a force enabler. Automation affects everything on the battlefield including combat vehicles, communication, weapons systems, intelligence gathering/processing, and command and control (Tyler, 1997). As such, these systems, which the military is becoming more dependent on, become a valuable target set and must be protected.

Increased reliance on and use of information systems is particularly true in the United States Air Force. Over the last 4 years, the Air Force placed great emphasis in modernizing and automating its command and control systems (Bearden, 2000). In fact, an entire organization has been established, the Aerospace Command and Control, Surveillance, Intelligence and Reconnaissance Center (AC2ISRC), with responsibilities for modernization planning, operational requirements, configuration control and Air Force requirements generation. Such modernized systems include the Global Command and Control System

3

(GCCS) and the Theater Battle Management Core System (TBMCS). These systems are designed to provide crucial information at the appropriate time and displayed in such a way to enable commanders at every level of war to better prosecute a conflict (Breaden, 2000).

The fact that commanders at all levels trust and rely on automated information systems for decision-making makes these systems prime targets for our adversaries. Tampering or disruption of such systems by an adversary can have serious implications on the battlefield. This disruption and or tampering, is termed offensive counter-information warfare (AFDD 2-5, 1998:9). By conducting Information Warfare (IW), an adversary can attempt to compromise tactical decision-making by making it difficult for decision-makers to assess situations and take appropriate actions. In addition, false or distorted information may fool a decision-maker into actions detrimental to his own forces.

The Air Force has experienced a steady increase in attacks against its information systems and experts agree that this trend will increase. These attacks are coming from a variety of attackers, from foreign intelligence services, to organized crime to malicious insiders (Fleeger, 2001). Much work has been done to mitigate the risk of such attacks to include the development of effective physical barriers such as firewalls and virtual private networks in addition to increased security awareness training for personnel (Mayer 2000). Despite the efforts, attacks continue.

Research by Bisantz et al., (2000) has indicated that IW may impact an individual's trust in and use of an automated information system by reducing the perceived reliability of information presented. As an individual's trust in a system decreases so does his use of the system's automation in favor of alternative means of task completion. Related research by Skita, Moiser & Burdick, (1996) involving unreliable information and the use of automated

aids, found, as the task demands of verifying unreliable information increased, the

subsequent use of automation increased. This was the case despite the level of information

reliability. Because of the serious consequences that may arise from relying on system

automation in situations where information presented may be unreliable, i.e. in military IW

environments, it is important to understand how decision-makers under varying levels of task

load may rely upon critical systems automation.

Problem Statement and Purpose of Research

The main purpose of this study was to begin to answer the following two questions:

First, is there a relationship between an individual's perceived trust in a system's automation

and his subsequent use of the automation? Second, does an individual's task load play a

moderating role in the relationship between trust and automation use? Both questions were

framed in an environment in which trust level was degraded; i.e., in an IW environment.

Factors that influence an individual's trust and subsequent use of automation in an

adversarial environment are important due to the unwanted and potentially dangerous

consequences that may occur when tampered information is utilized in critical decisions.

This is true not only for the United States Air Force, but for any organization that relies upon

information systems for critical decision-making.

Summary

The information age has brought about exciting advances in technology, especially in

the area of automation, that have produced great benefits in terms of increased efficiency and

productivity in areas such as finance, power control and information processing. These

benefits have resulted in increased use of and reliance on such technologies for critical

decision-making, thus producing increased liabilities in terms of vulnerabilities to interruption and deception. Because the vulnerabilities exist and are being exploited, it is important to understand the affects that exploiting these vulnerabilities have on the trust an individual places in these technologies and his resulting use of the technology for critical decision-making. This is especially true in the United States Air Force as it continues to increase its use of and reliance on such technologies for command and control decision-making in adversarial environments.

Thesis Organization

The following chapters present support for the model that was used to observe factors that may influence an individual's trust in an information systems automation and subsequent use during varying task load in an adversarial environment. Chapter II provides a literature review of the body of work in decision-making, command and control, information warfare, and trust in automation. Hypotheses are presented that were tested in an empirical experiment. Chapter III presents the experimental and methodological framework for the experiment used to test the hypotheses. Chapter IV presents the statistical analysis of the data collected from the experiment. Finally, Chapter V presents the research findings and conclusions.

II. LITERATURE REVIEW

Introduction

This chapter presents the literature reviewed for this study with the aim of providing the reader pertinent background information related to the human-information system trust relationship within the context of an adversarial command and control environment. The chapter begins by presenting information on the following theories and concepts: decision-making, command and control, information warfare, trust; including human-human trust, and human-computer trust, trust in automation and trust in an adversarial environment. Next, a trust model is presented based on the related literature. Finally, hypotheses are presented based on the trust model that relates constructs that may influence an individual's trust and subsequent use of systems automation.

Theories and Models of Decision-making

To understand the various factors that affect human's trust in information systems in a command and control environment, it is important to first understand how information systems are utilized in this venue. Today's military command and control systems give commanders the means to exercise authority and direct forces in accomplishment of the mission. Commanders "use information to support decision-making and coordinate actions that will influence friendly and enemy forces to the commanders advantage" (Joint Pub 6-0, 1995: I-2). In order to understand how decisions are made and what influences a decision-maker, a brief review of relevant decision-making processes and research was performed.

Decision – Making Processes

Decision-making methods can be broken down into two distinct terms: analytical and intuitive (Klein, 1988; Klein and Klinger 1991). Analytical methods are based on logical analysis of the decision situation while intuitive based decisions rely upon pattern recognition and experience. A good example illustrating both methods was the series of chess matches between chess master Gary Kasparov and the computer Deep Blue. "The computer used detailed and exhaustive option analysis to decide on each move while the chess master decided his moves based largely on knowledge, experience and recognition of patterns" (Bergstrand, 1997:1).

Rational Choice Model

Early research in decision-making, 1955 through 1975 was centered around analytical decision-making (Collyer and Malecki, 1998). One model, the Rational Choice Model is the baseline against which other models are compared (Allison, 1971). The rational choice model is based upon an economic view of decision-making. It is grounded on goals/objectives, alternatives, consequences, and optimality. The model assumes that complete information regarding the decision to be made is available and one correct conception of a problem, or decision to be made can be determined. In a strict sense, the rational model states that people choose among different alternatives by moving through a series of steps based upon their knowledge of the situation and the desirability of the outcomes (Simon, 1957). Collyer and Malecki (1998) and Klein (1988) point out that a major limitation with the rational model is the long time required to structure the decision problem and obtain judgments needed to derive a solution. March and Simon, (1958) also point out limitations in that the model makes the assumption that a decision can be made with

8

certainty, when in reality most decisions are made with uncertainty. The best times to use analytical decision-making are in situations with low time pressures, the need for careful documentation exists and in a context free task with many components (Klein, 1988).

Naturalistic Decision-making

For many years classical analytical decision-making theories, such as the rational approach, were accepted by most decision researches (Cannon-Bowers, Salas and Pruit, 1998). Since the mid 1980's, some researchers have turned their attention to the more intuitive approach toward decision-making, or naturalistic decision-making because, "it is not feasible to apply classical decision- making research analyses to many real life situations because it fails to account for decision-maker experience, task complexity, and the demands of the naturalistic environment" (Orasanu and Connolly, 1993:19). Researchers have moved away from the static environment of the laboratory and embarrassed a more naturalistic view involving the more complex real world and the systems in it. Researches have replaced college students in laboratories with experts and operators in their natural environments (Randal and Pugh, 1996; Collyer and Malecki, 1998). Naturalistic decision-making is derived from the study of how individuals make decisions in real situations in their natural environment. Klein (1993) provides a description of naturalistic decision-making and gives a description of the process as it occurs in the field. Naturalistic decision-making is characterized by dynamic and continually changing conditions and involves eight required setting characteristics (Orasanu and Connolly, 1993). These eight characteristics are shown in table 1 on the following page.

Table 1: Characteristics of Naturalistic Decision-Making Settings

Characteristics of Naturalistic Decision-Making Settings
• Ill-structured problems • Uncertain dynamic environments • Shifting or compelling goals • Action/feedback loops • Time stress • High stakes • Multiple players • Organizational goals and norms

Cannon-Bowers, Salas and Pruitt (1996) describe additional factors, among others, that help define naturalistic decision-making are multiple event feedback loops and time constraints. They propose that decisions in real environments are temporally dependent and ongoing with the outcome of iterative decisions affecting subsequent decisions and that time to decision is often critical to the success of the decision outcome. The concept of time, or speed in decision-making and iterative decisions support a similar concept that is part of Col John Boyd's Asymmetric Fast Transient theory of conflict, a subset of which is called the OODA loop. The OODA Loop was offered to explain how military commanders make decisions in a command and control environment (Fadock, Boyd and Warden, 1995).

Observation, Orientation Decision Action (OODA) Loop Theory

Boyd's OODA loop can be seen as a variation on the rational choice model of decision-making. The OODA loop model's premise is that decision-making is the result of rational behavior (Boyd, 1987). As such the process can be depicted as a cycle of four stages that describes the decision-making process of military commanders in C2 environments. Boyd's model is illustrated below in figure 1.

Observation   Orientation
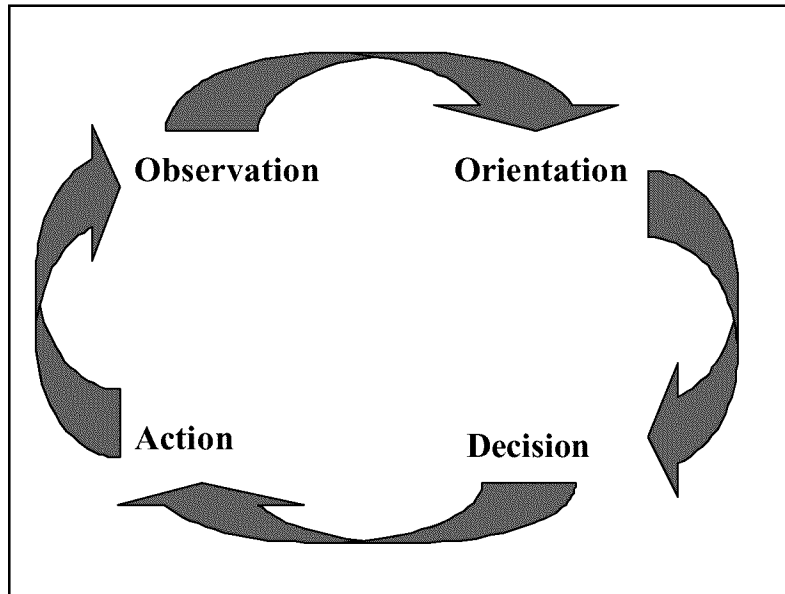
Action   Decision

Figure 1: The OODA Loop

The first stage of the OODA loop is observation. It is here where the decision-maker must

observe what is happening around him and determine the circumstances under which he must

function. He collects and synthesizes available data from a variety of means and sources to

obtain situational awareness, which occurs in the second stage, the orientation stage of the

loop.

Orientation is the next stage in the OODA loop. After the data is collected, it must be

synthesized into information by the decision-maker. This is where the decision-maker

orients himself to the information he observed by creating a mental picture of the world

around him (Fadock, 1995). Klein's (1998) Recognition-Primed Decision (RPD) model

supports this concept. It is in this stage that a decision-maker uses the information and his

own knowledge to recognize a situation as typical. The RPD model emphasizes the

importance of situation assessment in expert decision-making (Drillings and Serfaty, 1997).

The mental image, which is formed during orientation, and is influenced by the decision-makers experience or recognition serves as the foundation upon which a decision will occur.

Coming to a decision is the third stage in the OODA loop. Here the decision-maker weighs the information gathered, considers the alternative courses of action and makes a decision. This is consistent with the Rational Model. In stressful, complex, dynamic situations the element of time criticality is one of the most distinctive features of decision-making (O'Hare, 1992). The RPD model may provide an explanation as to why military commanders are able to make decisions faster than what would be considered normal using the rational choice model. RPD focuses on assessing the situation rather than considering multiple courses of action. More effort is said to be expended on understanding and assessing the situation, which results in a reasonably good course of action to take. In this way the decision-maker does not generate a list of options, they make a decision and act upon it as soon as the minimum information is acquired (Randel and Pugh, 1996).

The last stage in the OODA loop is the action stage. It is here where the decision-maker initiates some action or behavior based on the three previous stages. The action may include the decision not to act. Observation of the actions or inactions starts the cycle over again. The amount of time used by a decision-maker to cycle through the OODA loop is often referred to as the cycle speed or size of the loop. Boyd contends that one can paralyze an enemy by operating inside his OODA loop, in other words operating at a faster cycle time (Fadok, 1995).

This is demonstrated in the following statement:

> An engagement between two opposing sides can be seen as competition to possess the smallest OODA loop. The side with the smallest OODA loop operates at a much higher tempo, forcing the opposing side to react to its moves. Through a successful campaign of subversion, deception, and psychological operations, friendly forces can increase the size of an opponent's OODA loop, while reducing the size of their own (Crawford, 1995:5).

In Boyd's Asymmetric Fast Transient theory of conflict, the goal is to operate at a faster speed than your opponent can react. In other words, make better decisions at a faster pace than your adversary. Information warfare is one means by which an adversary can interrupt or impede the OODA loop process within a command and control environment. It is therefore important to understand the components involved within this command and control environment and how they may be disrupted in order to influence the OODA loop process and thus affect decision-making.

Decision Support Systems

Decision Support Systems (DSS) are one component within the command and control environment that may be taken advantage of by an adversary through the use of IW activities. DSS systems are used and designed for many types of organizations including hospitals, banks, insurance companies, and military organizations. A DDS system is an interactive computer based system that aids decision-makers in using stored data to solve ill-structured, unstructured, or semi-structured problems (Sprague and Carlson, 1982). Holsapple and Whinston (1996) describe five characteristics that should be observed in a DSS system. These five characteristics are: (1) DSS contains knowledge describing aspects of the decision-makers environment, that indicates how to accomplish a range of tasks, and that

indicates valid conclusions in different circumstances; (2) DSS has an ability to acquire and maintain descriptive knowledge as well as other kinds of knowledge as well; (3) DSS has an ability to present knowledge on an ad hoc basis in various customized ways as well as in standardized reports; (4) DSS has an ability to select any desired subset of stored knowledge for either presentation or deriving new knowledge in the course of problem recognition and/or problem solving; (5) DSS can interact directly with a decision-maker or a participant in a decision in such a way that the user has a flexible choice and sequence of knowledge-management activities. In general, a DSS must provide up-to-date, timely information that is complete and accurate and in an appropriate format which is easily understood and can be manipulated.

With the advent of the revolution in military affairs, and the reorganization of the Air Force into an Expeditionary Force, the United States Air Force has seen increasing use of information technology, including DSS, within its command and control environment to aid people in critical decisions. This is evident in extensive development and recent deployment of the Integrated Command and Control System (IC2S) block 00, which is a global network of software systems that links data bases, operations centers, sensors, and shooters, the core of which is the Theater Battle Management Core System (TBMCS) (AC2ISRC, 1999:3). Therefore, a review of command and control (C2) literature was performed in order to understand the role of C2 and establish a relationship between information systems and human trust in these systems.

Command and Control

Although there are many differing definitions of what C2 means, (James, 1999) the

Air Force defines command and control as, "The exercise of authority and direction by a

properly designated commander over assigned and attached forces in the accomplishment of

the mission" (AF Directory 33-303, 1999:14). Roman (1996) suggests the military adopt a

C2 organizational structure that promotes decentralized decision-making by eliminating

layers of command by flattening the organization hierarchy. He states that centralized

control by a hierarchical organization may no longer be possible in future fast tempo

conflicts. He believes information gathering and decision-making must be made at the level

in which the information is received, before that information is passed on to higher levels.

Roman believes, by allowing contact troops to make decisions based on first hand

information, a chaotic environment can be made less chaotic at higher levels due to a

decrease in the amount of information that needs to flow up the command hierarchy. The

modernization of the Air Force's C2 environment is allowing for more decentralized control

by leveraging modern technology that enables commanders at every level to better prosecute

a conflict (Bearden, 2000). With this switch from a more centralized control to more

decentralized control, commanders at all levels are becoming reliant on information systems

as a means to collect, analyze, and display real-time information from multiple sources and

sensors in order to make critical decisions about an evolving tactical situation. Dillion &

Morris (1996) suggest that trust in both the information system and the source of the

information helps determine the usefulness and value of such tools for the decision-maker.

Bisantz et al., (2000) proposed a framework for studying human trust in automated

decision-making aids in a C2 environment. Their study suggested that the threat of an attack

by an adversary against a C2 system was a significant factor that influenced decision-making in a C2 environment. It is therefore beneficial to take a look at the literature on this unique-military threat known as Information Warfare.

Information Warfare

Information Warfare (IW) is an often-used buzzword in today's military circles. The concept is based on the fact that information and information technologies are becoming increasingly important to our national security. Information warfare research is a top priority of the Department of Defense (Myers, 1999). Although a hot topic today, information, and its use has always been a critical factor in times of war. According to Clausewitz, "imperfect knowledge of the situation…can bring military action to a standstill" (Howard and Paret, 1976:56). Sun Tzu in 500 B.C., talked a great deal about the value of information, he believed it was inherent in war fighting. Deception, a form of misinformation, was one of Sun Tzu'z tenets of warfare (Sun Tzu, 1983). It may be obvious that the more a force knows about itself and its enemy, the stronger that force will be in times of battle. What is less obvious are the varying uses of the available information and how it can be manipulated to reinforce or weaken the strength of a fighting force. In times past, information gathering, deception and battles required enemies to be in close proximity of one another. With the modern complexities of war and the ensuing information technological advances, these activities can now be employed from a great distance, with varying techniques and with anonymity. An enemy, as well as our own forces, can now attack critical information systems for varying results, using a wide variety of techniques. Hence, it is important to

understand which of these techniques may affect a military decision-maker's trust in the C2 information systems they rely upon.

What is information warfare? Libicki (1995), describes coming to grips with a definition is like the proverbial effort of the blind men to discover the nature of the elephant: the one who touched its leg described it as a tree, the one who touched its tail called it a rope, etc. The literature groups IW into two broad categories; one that sees the use of IW to support decision-making and combat operations while the other regards information as a weapon in warfare (Whitehead, 1997). The Air Force defines information warfare as "any action to deny, exploit corrupt or destroy the enemy's information and its functions while protecting Air Force assets against those actions and exploiting its own military information operations" (Joint Publication 3-13.1, 1998:3). The Chinese definition of information warfare is similar to the Air Forces. The Chinese define IW as the "use of firepower and command to obtain and to deny information, to suppress and counter suppress, and to deceive and counter deceive, as well as to destroy and counter the destruction of sources of information" (Mengxiong, 1995:16). Joint Publication 3-13.1 (1998) describes an application of IW that employs various techniques and technologies to attack or protect a specific target set, command and control, called Command and Control Warfare (C2W). C2W integrates the use of military deception, psychological operations, operations security, and physical destruction, all supported by intelligence, with the aim of denying information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions.

Information Manipulation Theory

As in Sun Tzu's time, deception with an aim of influencing decisions, is still a key component in IW operations. The Air Force uses C2 technologies (information systems) increasingly in a variety of ways, from managing and moving supplies and troops to monitoring and tracking enemy movements to weapons targeting and acquisition. The intentional manipulation or spoofing of these information systems poses a great threat to military command and control decision-makers (Kuel, 2000). Imagine if one could alter the information on quantities of critical supplies being shipped to a certain location, the coordinates of critical intelligence buildings, or an Air Tasking Order that sent a flight of aircraft to a target that was not there or was something different than what was expected. Recall the fallout from the mistaken NATO bombing of the Chinese Embassy in Belgrade in 1999. The U.S. and Britain contend that the bombing was the result of intelligence sources having used an old and unreliable map (Marsden, 2001). Imagine a scenario where a rouge nation manipulates information in a U.S. command and control center that causes an unplanned incident or series of incidents such as the Chinese embassy bombing. Such action could facilitate the undesired (from the U.S. perspective) conflict between nations. The potential damage caused by an adversary by creating false information in our command and control systems is enormous.

McCornack, Levine, Morrison, and Lapinski (1996) introduced the theory of information manipulation to describe deception in communication. This theory suggests that violation of one or more of the maxims (quantity, quality, relation, and manner) results in a deceptive communication. For example, the intentional manipulation of the number and type of aircraft at a particular airbase in a C2 information system violates the maxim of quality

and, therefore would be classified as information manipulation. This theory also suggests that the intentional manipulation of information may influence a decision-maker to make a decision that is different from what he would have made given the original information.

Because information warfare is a threat and command and control environments, such as Air Operations Centers, are increasingly reliant upon automated information systems to aid decision-makers in critical decisions, there is potential for adversarial forces to tamper with and disrupt such tools. Llinas et al., (1998) indicate information warfare can impact an adversary's operation through information disruption, denial, and distortion. These means can make it difficult for a decision-maker to assess situations and take appropriate action as well as cause or fool them into taking actions undesirable actions. Given the potential for IW to corrupt and disrupt information provided by automated information systems it is important to understand to what extent decision-makers rely on and use these systems and what factors may influence an individual's trust in such systems.

Trust Definitions and Concepts

Nass, Fogg and Moon (1996) and others, have found that the trust relationship between humans and computers is similar to the trust relationship that humans have between each other. Many of social rules and dynamics, which guide behavior in human interactions, also apply to human-computer interactions. Given this finding, it may be assumed that antecedents of trust in human-computer interaction are likely to be the same as antecedents of trust between humans. Definitions of trust, as it applies in human-computer interactions, are drawn from definitions of trust developed to apply to human relationships (Muir, 1998). The word trust is so frequently used in our everyday language that most sources assume the

audience knows what it means and thus is rarely defined. When it is defined within scholarly literature however, definitions form a wide range of meanings (McKnight and Chervany, 1996). Before talking specifically about research regarding trust in automation, a brief review of the meaning and concepts of trust is presented.

Common definitions of trust mainly concentrate on interpersonal aspects rather than on trust in social or technical systems and also tend to focus on personal sources, effects of trust or behavioral aspects. Evidence of this can be seen in Webster's Third New International Dictionary (1993) as it defines trust as follows: (1) Assured reliance on a person or thing, (2) Dependence on something future or contingent, (3) An equitable right or interest, (4) A charge or a duty imposed in faith or confidence or as a condition of some relationship, something committed or entrusted to one to be used or cared for in the interest of another. There are additional definitions that can be used to examine trust in automation from a human factors perspective which are more specific to trust in human relationships than Webster's definitions. Barber (1983) a sociologist, recognizes trust as having multi-dimensional characteristics and defines trust in terms of three specific expectations: persistence of natural and moral laws, technically competent performance, and fiduciary obligations and responsibility.

Trust is also a dynamic construct that changes over time as experience in the relationship grows. Zanna (1985) suggested that trust between individuals has dynamic characteristics and regards trust as a generalized expectation that undergoes predictable changes as a result of experience in a relationship. The three characteristics are: predictability, dependability, and faith and can be seen as representing stages in a relationship (Remple et al., 1985). Predictability, which forms the basis of trust early in a

relationship, is built on predictability of behaviors and therefore, built on observable factors. As the relationship matures, trust comes to rest on dependability. It is based on the attribution of the qualities and characteristics of the trusted individual. Finally, growth of trust depends on a leap of faith because one cannot determine dependability of behaviors in future situations, which have yet been exhibited (Llinas et al., 1998; Remple et al., 1985).

While the discussion above represents classifications of trust related to human – human relationships, Sheridan (1988) offered additional attributes of trust in the realm of human- computer relationships. Sheridan examined how trust affects an operator's use, or non-use of an automated aid when the opportunity arises. Sheridan suggested seven attributes of trust in command and control systems: *Reliability*, which implies the reliable, predictable, and consistent functioning of a system; *Robustness*, is the demonstrated or promised ability of a system to perform in a variety of conditions and circumstances; *Familiarity*, is the feeling of being comfortable with your ability to deal with a situation or object despite there being a high degree of novelty associated with it; *Understandability*, has to do with ones ability to develop an appropriate mental model of the situation, possibly with the aid of familiarity; *Explication of Intention,* rather than leaving a person in a position of having to understand and discover covert meanings from a system's behavior, this attribute allows people to trust others over those who just perform tasks; *Usefulness*, this attribute defines the level at which data or machines respond in a useful way that creates something of value for system users; *Dependency*, is the level to which an operator is willing to depend on a machine. It is from these definitions, characteristics and attributes that trust models have been developed and subsequent research in the area of human trust in automated information

systems and decision aids has been conducted. (e.g. Zuboff, 1988; Lee and Moray, 1992;

Muir and Moray, 1996; Sheridan, 1988; Skitka, Mosier, and Burdick, 2000).

Trust in Automation Research

Zuboff (1988) studied how people trust automated systems in the workplace. The

research found that people tended to distrust the technology of the automated system and thus

used the system less or that they tended to over trust the system, which resulted in other

problems when the system failed. Other empirical studies, consistent with Zuboff's, have

shown that people's strategies with regards to the use or non-use of automated aids may be

affected by their trust in the system. Muir (1987) developed a hypothetical model of human

–machine trust, which consisted of the linear combination of characteristics that Barber

(1983) outlined. Muir's model depicted human trust by the combination of persistence of

predictable behavior, technically competent performance, fiduciary responsibility, and the

interaction between these characteristics.

By conducting a series of experiments on a continuous chemical process control

simulation, Lee and Morray (1992) and Muir and Morray (1996) extended earlier work by

Muir and developed a dynamic model of trust. They produced a model depicting that an

individual's current level of trust was affected by his previous level of trust as well as system

factors such as the existence of automation faults and system performance. In other words,

this model incorporated the additional characteristics of predictability, dependability, and

faith as explored by Zanna (1985) but related them to the human – computer trust

relationship developed by Muir. These studies found that workers monitoring the automated

systems became complacent when the system was perceived to perform correctly, and that

workers who perceived the system was prone to errors spent more time monitoring the system. In addition, the studies showed that an operator's decision to use the automation or manual control's depended on his perceived reliability of the automated system (trust in the system), as well as his perceived reliability of manual control (trust in self) to manage the system. There was a very high correlation between an individual's trust and the use of automation. These studies also produced evidence that suggests that once an individual perceives an error in the automation, his trust in the system will degrade for a period of time and then gradually rebound over time.

Automation Bias

More recent studies in the use of automation that are consistent with Zuboff's (1988) study and those of Muir and others describe phenomena called the automation bias. (e.g., Mosier, Skitka, Heers & Burdick, 1997, 1998; Skitka, Mosier & Burdick, 1999). Automation bias is the " tendency to use automation as a heuristic replacement for vigilant information seeking and processing" (Skitka, Mosier & Burdick, 1999). In other words, the tendency for a decision-maker to over-rely on automation to perform tasks and make decisions rather than using the automated aid as one component of the decision-making process. Theses studies identified two classes of errors that routinely emerge in highly automated decision environments, these being omission errors and commission errors. Omission errors are defined as, "failures to respond to system irregularities or events when automated devices fail to detect or indicate them," and commission errors as "errors which occur when people incorrectly follow an automated directive or recommendation, without verifying it against other available information" (Skitka and Moiser, 1999: 344). A Conejo and Wickens (1997) study involving an Army threat target recognition tool, provides a good

example of a commission error. They found that on occasion when an automated cue was unreliable, directing attention to something that was not the designated target, pilots were still very likely to choose the non-target as the target, despite the fact that the true target was known to the pilot and visible on the system display. These studies provide evidence that automation bias exits and may be due to excessive reliance on trusted automated systems.

Truth Bias

Automation bias is similar to another phenomena described by McCornack et al., (1996) called truth bias. Truth bias suggests that as a trusted relationship develops between individuals, they are apt to believe information given to them by others in the relationship without verifying the information. Biros (1998) extended McCornack's truth bias theory to include an individual's trust in artifacts generated by an information system as he examined the effects of information manipulation through his proposed artifact truth bias model. Automation bias, truth bias and artifact truth bias provide additional support to the findings of Nass, Fogg and Moon (1996) that suggest that individuals trust information systems in the same way as individuals trust others. In addition, automation bias and artifact truth bias provide support to the notion that decision-makers who rely on and trust information systems may be vulnerable to certain aspects of information warfare.

Automated Aids in an Adversarial Environment

The studies mentioned above provide a good foundation for continued research in the area of human-computer trust but are limited in the fact that they have dealt with situations where human trust was measured in terms of the behavior of the automated system with regards to its predictability, dependability and the user's faith in the system in a benign process control environment. A military command and control environment adds additional

facets to the trust relationship in that the automated system is open to deliberate manipulation by an enemy. Human operators must not only deal with mechanistic failures, but also predetermined deception or misguidance perpetrated by an adversary. Research in this military unique situation was, until recently, non-existent.

The majority of research conducted has been by a team of researches at the Center for Multi-source Information Fusion Department of Industrial Engineering at State University of New York at Buffalo. (e.g. Llinas et al.,1998; Biasntz et al., 2000) Three phases of research have been conducted to date. The first phase consisted of a comprehensive literature review and discussion, which focused on "defining, characterizing, and modeling the dependences and vulnerabilities of aided-adversarial decision-making (AADM) on components of information" (Bisantz et al., 2000:1). (Aided-adversarial decision-making refers to decision-making by military personnel with computerized aids in an environment where there is the potential for information warfare activities by an adversary to corrupt the decision aids) During phase one, in order to investigate the human-computer trust relationship in this more specific situation of AADM, Llinas et al., (1998) proposed a Lens Model approach, as shown in Figure 2, for the modeling of human trust in automated systems.
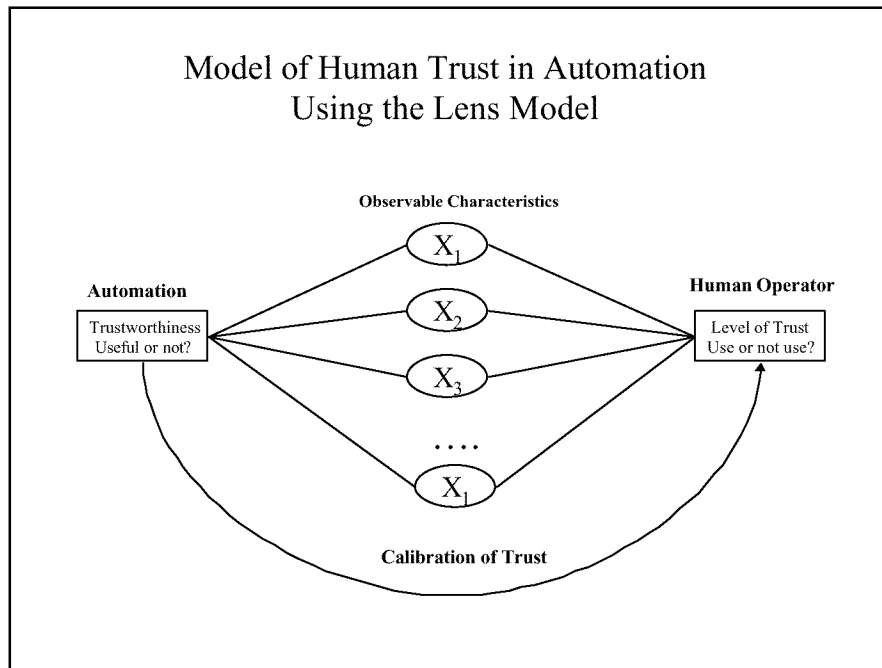
Figure 2: Adapted Lens Model of Human Trust in Automation

They felt the lens model provided a means "for modeling both human judgment policy and the actual structure of the environment, it allows operator calibration to the actual trustworthiness of a system to be explicitly considered" (Llinas et al., 1998:99). Observable cues (characteristics), which an operator would use to make a judgment, may include the characteristics and components of trust as described by Sheridan (1988) and others. For example, predictability, dependability, faith, and reliability may be cues used. During phase two an experimental framework was established to evaluate the lens model approach in an information warfare environment. In this environment trust was considered in the context of adversarial decision-making in which information may be intentionally altered or degraded by an adversary (Seong, Llinas, Durry, and Bisantz, 1999). In addition to the development of a framework for experimentation, an empirically based, multi-dimensional scale of trust,

26

which could be used for the purposes of measuring an individual's feeling of trust in an automated system was developed. In developing the trust scale, the authors found empirical evidence that the concepts of trust and distrust were opposites and that one scale can be used to measure both. In addition, the study found that concepts of general trust, human-human trust, and human-machine trust were similar (Jian et al., 1998).

The third phase of the research involved initial empirical investigation into the trust-related vulnerabilities of AADM. The investigations were built upon the experimental framework and trust measurement scale developed in the prior phase as well as the development of an experimental test-bed in which experiments could be run on (Bisantz et al., 2000). The initial experiment was conducted to assess how an individual's decision performance and selection of information (implying trust in the system) were affected by different system failure causes. (i.e. sabotage, hardware/software failure, or unspecified). Results of the experiment indicated that different fault causes (i.e. information warfare) may impact an individual's trust in and use of an automated information system. In addition, results showed that the trust scale developed in phase two of the research could be used to identify differences in the level of trust as system and environmental conditions varied. The framework and trust scale developed as well as the data gathered in theses three phases of research, provide a good source of information and data for future research to use and compare to.

Another recently completed study in this area, Fields (2001), focused on the effect external safeguards have on an individual's trust in a system in an information warfare environment. In this study, participants were immersed into a complex command and control

scenario using a high-fidelity computer simulation in order to measure the effects of the following variables; external safeguards and information warfare on trusting behavior.
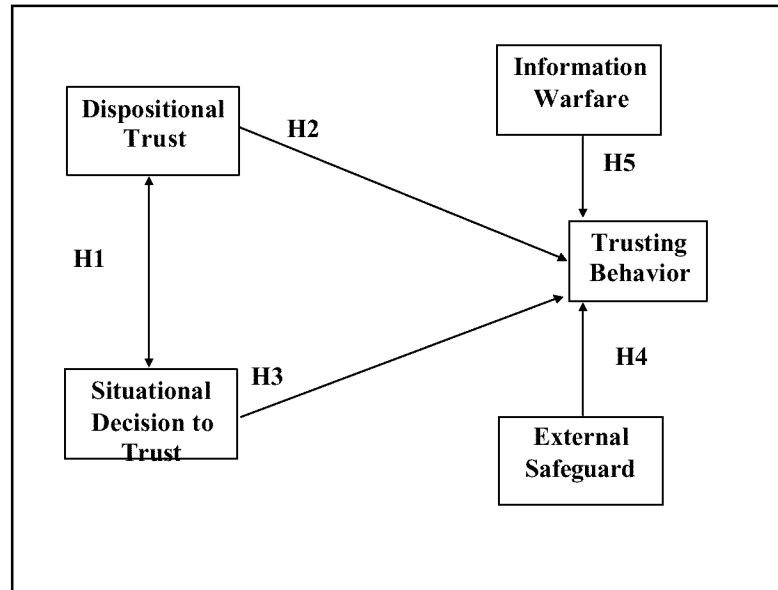

Figure 3: Fields Adapted Model of Trust

Using the above adapted model of trust drawn form McKnight and Chervaney (1996) Fields hypothesized, among other things, that external safeguards would have a positive effect on trusting behavior and that the presence of information manipulation will have a negative effect on trusting behavior. Although not conclusive, and one that bears further investigation, Fields' study showed a negative effect on trusting behavior when external safeguards were high. In addition, results indicated that a perceived information warfare attack had no effect on an individual's trusting behavior. A factor that may have influenced whether an individual tried to verify possible suspect information when they perceived an information warfare attack is task load. Subjects indicated that they were so busy concentrating on performing the required task that they either did not have time to contact a

verification source or they had forgotten about the option to contact a verification source.

Task load may have played a role in the participant's loss of complete situational awareness.

Task Load and Situational Awareness

Situational Awareness (SA) is the decision-maker's moment-by-moment ability to monitor and understand the state of a complex system and its environment (occurs in the orientation stage of Boyd's OODA loop). The completeness and accuracy of decision-makers situational awareness' is crucial to the ability to make decisions during emergences (Wickens, 1998). To maintain an accurate SA the decision-maker should take into account both information that is available and that which can be activated from memory (Lyons, 2000). In a high task environment, when a decision-maker is confronted with several threats, memory load can quickly become overloaded (Lyons, 2000). This memory overload can cause an individual to begin to dismiss important cues, existing and past, from the environment (Weick, 1995). This situation of increased workload and its effects can cause a decrease in situation awareness as depicted in Wickens, Mavor, Parasuraman, and McGees's (1998) model of failure recovery in air traffic control shown in figure 4 below.
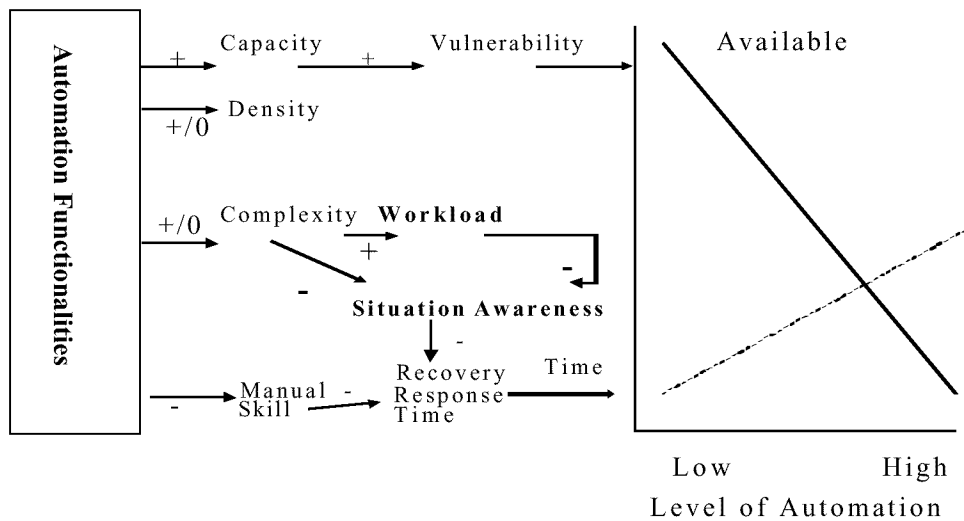
Figure 4: Model of Failure Recovery in Air Traffic Control

The presence of information warfare activities may be one such critical cue

dismissed by an individual in a high task environment and the dismissal of which may result

in an undesirable decision being made.

Task load may also play a role in the negative effects of automation bias by

individual's committing automation commission errors, i.e., errors made when an individual

takes an inappropriate action due to over reliance on automated information or direction. As

task load increases, individuals may rely more on automation, even in situations in which the

automation may not be reliable. Skitka, Mosier and Burdick (1999), conducting a study

involving the use of automated monitoring aids in situations where information presented

may be unreliable, found that task load had an affect on whether individuals used system

automation or not. As the demands of verifying the information increased, individuals

decreased their verification efforts and used the systems automation more. In general, when

given a choice, individuals tend to prefer options that require lower investments in terms of attention and effort. Weick (1995) contends that as "arousal (i.e. workload) increases, people tend to abandon recently learned responses and categories and fall back on earlier, over learned, often simpler responses" (Weick, 1995:102). When individuals have come to trust system automation, and have come accustomed to using it, a high task load environment may cause them to overuse the automation even though it may not be reliable.

Research Hypotheses

The literature and studies on human-human trust relationships; human-computer relationships and human-computer trust relationships in adversarial relationships all provide possible trust models from which hypotheses may be proposed. The hypothesis proposed in this section are based on a model composed of relationships taken form Muir and Morray's (1996) dynamic model of trust, Llinas et al., (1998), lens model approach and Fields (2001) adapted model of trust and is depicted in Figure 5 below.
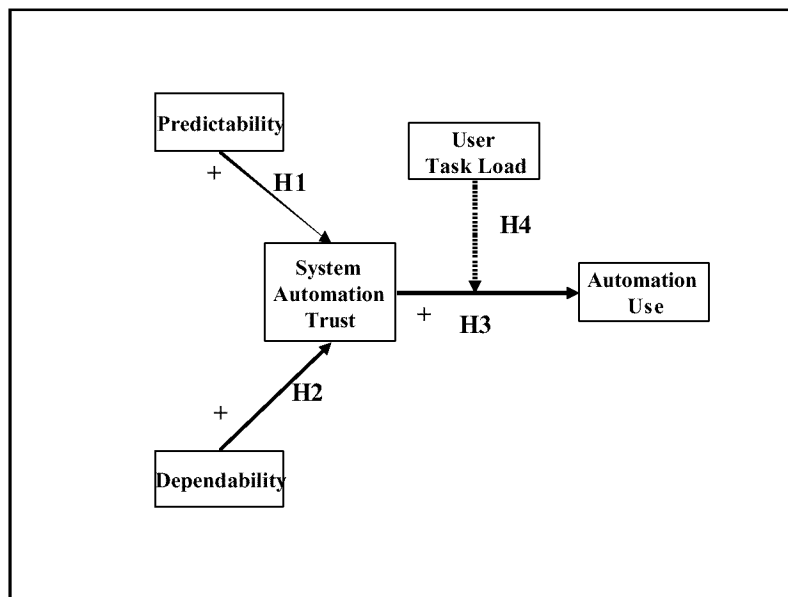

Figure 5: Developed Trust and Use Model

In this model, dependability and predictability contribute to an individual's overall trust in a system's automation. System trust then leads to use of system automation. User task load acts as a moderating variable between system automation trust and automation use and was used to test the affect this construct has on a decision-makers use of available automation. With this model *dependability* is defined as having the trait of being dependable; yielding the same or compatible results in different experiments or statistical trials. *Predictability* is defined as the ability to foretell (declare or indicate in advance) on the basis of observation or experience. *System automation trust* is defined as having confidence in and to entrust the system automation to do the appropriate action. *Task load* is defined to mean the level of workload of an individual throughout the course of the experimental simulation. (i.e. the number of resources an individual is responsible for and the number of enemy resources that need to be accounted for during the experiment simulation.) For the purpose of this study *automation use* is defined as the accomplishment of a task via system automation features in lieu of manual system techniques (i.e. using a system feature to accomplish many similar tasks simultaneously rather than completing each task individually in a more deliberate manner).

Hypothesis Development

The literature has demonstrated that trust is a multidimensional and dynamic construct that changes over time (Muir, 1987; Muir, 1994; Remple, Holmes & Zanna, 1985). Trust starts with the foundation of predictability built on observable factors, which demonstrated over time lead to a perception of dependability. In the latter stages, because one cannot determine dependability of future behavior that has not been exhibited, trust

depends on a leap of faith. In human-computer relationships, faith is based on the past perceived predictability and dependability (Lee and Morray, 1992; Muir and Morray, 1996; Muir, 1987). In an information warfare environment, it appears intuitive that observable and situational indications of IW activities would decrease the perception of predictability and dependability. Therefore, the following is predicted:

Hypothesis 1: Perceptions of predictability of system automation will be positively correlated with ratings of trust.

Hypothesis 2: Perceptions of dependability of an automated information system will be positively correlated with ratings of trust.

Individual users who trust technology are more inclined to utilize it for the purpose and in the manner in which it was designed (Muir, 1987; Lee and Moray, 1994; Seong, Llinas, Dury and Bisantz, 1999). The introduction of automated technology has changed the roles of human operators from that of direct computer control to management of differing levels of computer control. Individuals must know how to interact with system automation, know when to rely on it and know when to intervene in the process when it is suspect (Seong, Bisantz, 1998). Sheridan (1980) emphasizes that an individual's trust in automation plays a key role in determining the level of reliance a user places on automation. It has been demonstrated that low trust in automation delays it use (Riley, 1996). This study therefore, proposes the following:

Hypothesis 3: Trust in system automation will be positively correlated with use of system automation.

Even if hypothesis 3 holds, there may be circumstances that automation use will not decline even when trust in the system automation is suspect. One of these circumstances may be that of user task load. As the task load increases and more environmental cues are

being interjected into the environment, the individual may begin to resort to using the automation as a means of keeping up with the environment. The increased task load may be causing a decreased state of situational awareness and thus environmental cues, such as information warfare indicators, may be forgotten or ignored (Weick, 1995). Based on the above, it is expected that:

> **Hypothesis 4: User task load will have a moderating effect on the relationship between system automation trust and use of system automation.**

Summary

In summary, the goal of this research is to examine an individual's trust in system automation and subsequent use of that automation and to determine if automation use is affected by the decision-makers task load in a naturalistic decision-making environment. To examine these effects, an experimental design, based on the model presented in this chapter, is presented in the next chapter. Chapter III will operationalize the constructs presented in this chapter and present a methodology that was used to capture data pertinent to test the hypotheses presented herein. Finally, the methodology incorporates the characteristics necessary to create a naturalistic military decision-making environment.

III.   Methodology

Overview

The first chapter of this thesis described the research problem being investigated in this study. The second chapter provided a review of pertinent literature relating to the human-information system trust relationship within the context of an adversarial environment from which a model on system trust and automation use was developed. In addition, a set of hypotheses was offered to predict user trust and automation use in varying situations. This third chapter describes the methodology used in an experiment to test the hypotheses, operationalizes the constructs of interest, 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 that were used to make inferences about the data.

Experiment Method

In order to investigate an individual's trust and subsequent use of automation, an experiment was designed around a military command and control (C2) scenario that was used with a high-fidelity computer simulation, the AWACS Weapons Director Trainer (AWDT) developed by 21st Century Systems, Inc. This system allows subjects to be immersed into a military C2 micro-world. Computer simulations provide a conduit between laboratory and field experiments by providing a more realistic and natural environment. The use of micro-world simulations provides for greater experimental control. Despite being conducted in a laboratory setting, the AWDT system simulates a real-world decision-making environment that may be experienced by weapons directors on board E-3 Airborne Warning and Control System (AWACS) aircraft. Several crews aboard the AWACS coordinate their

efforts to provide airborne surveillance, and command, control and communications functions for tactical and air defense forces. Weapons directors are responsible for directing airborne assets, detecting, identifying, tracking and intercepting airborne threats, as well as conducting search and rescue missions, should the need arise. The AWDT system allows for the collection of quantitative measures over the course of each experimental session as well as providing a mechanism for collecting measurable attitudes an beliefs through survey questionnaires. The system also has the capability to capture and record actions of participants as well as measure an individual's task load throughout a simulation session.

Participants

Participants consisted of 40 Air Force Institute of Technology graduate students with military ranks of 2nd Lieutenant through Major along with Junior and Senior members of the Air Force ROTC detachment at Wright State University, with education levels ranging from, undergraduate to graduate. Both female and male participants participated. A majority of participants liked using computers and were comfortable with their use in the Air Force. All participants indicated in the Post Simulation Evaluation Sheet (see Appendix E), that the training provided was sufficient to use the system and that the simulation was easy to understand. In addition, over half the participants indicated verbally that they would like to "play the game again." These comments were in line with the experimenter's observation that all subjects appeared engaged during the treatment scenarios. All participants arrived in military uniform to help in portraying a military environment. All participants completed the experiment.

Experiment Design

An experiment was designed as a between-group experiment that manipulated two independent variables, Information Warfare and User Task Load. Implied IW will provide an environment in which system automation will be in question, thus providing a basis for potential decreased trust in the system automation. These variables were completely crossed in a 2 x 2 design configuration as shown in Figure 6 below. Each participant experienced only one of the four possible conditions.
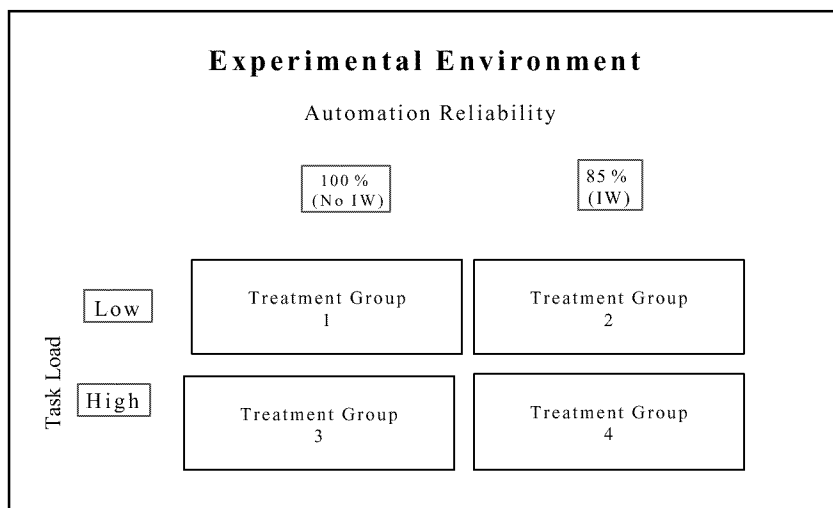

Experimental Environment

Automation Reliability

	100 % (No IW)	85 % (IW)
Low	Treatment Group 1	Treatment Group 2
High	Treatment Group 3	Treatment Group 4

Task Load

Figure 6: Experimental Group Configurations

Each participant was given training on the simulator concept and computer interface. A further description of the training is presented in the Task and Procedures section of this chapter. After completion of training, each participant was tasked to perform a hidden-profile, decision-making task that involved controlling multiple aircraft types to defend an area of operation and attack when possible in a simulated battle space. Control of the aircraft types was performed through various user actions on the AWDT system. The AWDT system

was described to the subjects as a new AWACS component undergoing initial testing by Air Force Research Laboratories.

Subjects were tasked to direct air assets against enemy assets with the aim of eliminating all threats in the area of operation. In addition, subjects had the opportunity to attack enemy positions as resources allowed. Subjects had the option to direct their assets using manual controls or to accept system recommendations that then automatically direct their assets. Manual direction of assets requires a minimum of three mouse clicks and manual positioning using the mouse. Automatic direction of assets could be accomplished by either clicking each visual representation of the current recommendations within an allotted time frame or by clicking a menu item that will accept all current active recommendations. (i.e., more that one recommendation can be accepted at a time.)

Subjects were told that system recommendations are derived from sophisticated algorithms designed with the aid of experienced AWACS Weapon Directors. Subjects can assume that recommendations are designed to best utilize existing resources while attempting to eliminate the highest occurring threat. Subjects were told that they could view their scores at anytime during the scenario. Scores were generated automatically by the system by taking the weighted sum of all eliminated enemy assets minus the weighted sum of the subject's assets destroyed. A positive score indicates that the value of enemy resources destroyed is greater than the value of the subject's resources destroyed while a negative score indicates the opposite.

Equipment and Environment

All experiment sessions were conducted in an office with no windows and a single entrance. Each subject performed his task in a designated workspace in which he was unable to see another's computer display unless he turned to look at it. Each subject's workspace consisted of a chair, a desk surface, and a PC computer with Pentium II 350 MHZ processor, 500 Meg of RAM, the Windows 2000 Professional operating system, and a 19-inch color monitor. Each system was loaded with the AWDT system software. Also included were quick-reference sheets, posted on the wall in front of the participants, that defined system icons and provided information about the values of all resources depicted in the simulation.

Task and Procedures

Experimental sessions were conducted over a four-week period in which the 40 participants participated in one of four treatment groups. Each experimental session lasted approximately 2 hours (see Figure 7) and used two or three participants.
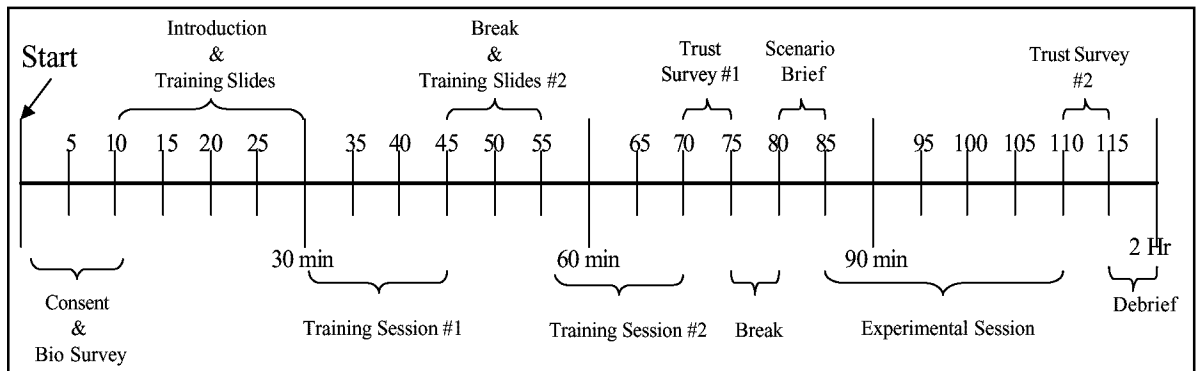
Figure 7: Experimental Time-Line

On their scheduled day (picked by the subjects themselves from various two-hour blocks throughout a four week period), subjects were instructed to report to the evaluation area located in AFIT Bldg 640, room 274. Subjects were assigned to a treatment group and

operator position based on a randomized block design (see Appendix G) based on the order

in which they arrived. Upon arrival, each subject was asked to sign a login sheet and

directed to an operator position. An experiment package was provided to each subject, part

of which included a standard consent form and a biometric data collection form (see

Appendix A). During the first five minutes, subjects were asked to fill out these two forms

before training began.

The experiment facilitator (reading from a script) started the session by explaining the

fictional purpose of the experiment (to evaluate some human factors issues regarding a new

piece of software for the AWACS aircraft). Next, the facilitator went through a PowerPoint

training presentation (see Appendix H) on a desktop PC located in the room. Following the

PowerPoint training session, subjects were given the opportunity to ask questions. The

experiment facilitator then started the first training simulation and instructed the subjects to

focus on practicing the actions learned during training and not be concentrating on getting a

good score. Subjects, if necessary, were individually shown how to perform the various

functions needed to operate the system. The experiment facilitator freely answered any

questions during this time. This first training simulation lasted approximately 15 minutes.

Following the first training simulation, the subjects were allowed a five-minute break while

the experiment facilitator reset the system for the next training session. After the break, the

experiment facilitator provided additional training via a PowerPoint presentation. During

this session subjects were introduced to the agent recommendation functions available in the

AWDT system. Following this brief period of instruction, the experiment facilitator again

answered any questions and then started the second and final training simulation, which

lasted 15 minutes. Again, the experiment facilitator provided assistance to subjects on proper

system operation and game play rules. Following this second training session, subjects were given the system automation trust survey to complete (See Appendix B.) They were instructed to put the completed form in the blue folders provided at each station. They were then allowed to take another 5-minute break.

Following the break, the experiment facilitator instructed the subjects to read the appropriate scenario brief (see Appendices C & D) and wait for further instructions. Subjects were instructed to raise their hands to request assistance if they encountered a computer malfunction or procedural question during the simulation. Subjects were also instructed to remain at their workstation at the completion of the experiment until otherwise directed by the experimental facilitator. Once all subjects indicated they were ready to begin, the facilitator started the final simulation and instructed the subjects to begin.

When the simulation ended the experiment facilitator passed out the second trust survey (same as the first one) and instructed the subjects to complete it and place it into the folder at their station and wait until all of the other subjects were finished. Once all subjects were finished, the experiment facilitator revealed the true purpose of the experiment. Participants were instructed not to discuss the experiment with others planning to participate.

Experiment Manipulations

The first experimental manipulation was the construct called Information Warfare (IW). It has been shown that indications of IW may reduce the level of trust individuals have in the automated system they are using (Bisantz et al., 2000; Fields 2001). IW was operationalized by planting the idea of IW in the minds of participants via the scenario description. The scenario revealed that the system had been down for a time due to an IW

attack, but presently the system was up and working but the reliability of systems

recommendations were in question (see Appendix C for full scenario). Treatment groups two

and four were subjected to the IW manipulation during the simulation. Groups one and three

read a similar scenario, but no IW or equipment problems were indicated (see Appendix D

for full scenario).

The second manipulation, User Task Load, was operationalized by increasing the

number of resources a participant was responsible for, along with the number of resources

used by the attacking force. Task load was increased by a factor of approximately 2.5.

Treatment groups one and two were subjected to a low task load, while treatment groups

three and four were subjected to high task loads. The load measure file, automatically

generated during the simulation, verified the task load of the individuals. Of the 20

individuals in the low-task load groups, 90 % indicated, on the Post Simulation Evaluation

Sheet (see Appendix E), that they felt the scenario was low-task load, while, of the 20

individuals in the high-task load groups, 85 % indicated they felt the scenario was high task

load.

Hypothesis Measures

In Chapter II a set of hypotheses was developed suggesting that the constructs of,

system predictability and dependability would affect users' perceived level of trust in a

system's automation, and that the perceived level of trust would impact their subsequent use

of the system's automation. In addition, it was hypothesized that an increase in user task

load would have a moderating effect on the relationship between automation trust and user

use of system automation. This section explains the procedures and instruments used to measure and collect data relating to these different constructs of interest.

Because cognitive phenomena like attitudes, motivations, expectations, intentions, and preferences are difficult to observe, a questionnaire (see appendix B) was used to measure the specific constructs of interest including trust, predictability, and dependability. This questionnaire is a derivative of one obtained from researchers at the University of South Florida (USF) which was developed specifically for the use of measuring the above mentioned constructs, as well as others, by actual weapons directors using the AWDT system. Credibility of the original questionnaire from USF was established using a Q-Sort analysis using six subject matter experts. The reliability analysis produced an alpha = .75 for predictability and .85 for trust. Dependability had no associated alpha, as it is a single item (Hoffman, 2000). All constructs were measured on a 6 pt. Likert-type scale in an attempt to force agreement or disagreement with each item and avoid neutrality. The scale ranged from 1 (Very Strongly Disagree) on the left to 6 (Very Strongly Agree) on the right. Questions one through seven dealt with the construct of trust, questions eight through ten dealt with the construct of predictability, and question eleven dealt with the construct of dependability. The survey was administered after the second training session and again after the final experimental simulation. The survey administered after the second training session served as a baseline to measure the overall trust individuals placed in the system's automation before any treatment was applied.

Automation use was measured by determining the number of times a subject accepted system recommendations vs. the number of recommendations issued. The act of depending largely on the system may be an indicator and measure of trusting behavior. The AWDT

system allows for the collection of this measure through automated data capture. The system can provide information on the number of recommendations given, whether the recommendations were accepted, and the manner in which they were accepted. (i.e., an individual recommendation was accepted or a group of recommendations were accepted.)

Analysis of the data collected during the experimental session was done through a variety of parametric statistical analyses methods. Pearson correlation analysis was performed to test hypotheses 1, 2, and 3, while analysis of variance (ANOVA) was used to investigate the difference in automation use between the environmental conditions of IW and Non-IW (high and low trust environments) as well as between the various participant task loads. In addition, ANOVA was used to determine if user task load has a moderating effect on the relationship between system automation trust and use of system automation.

Summary

This chapter described a research method to investigate the theorized relationship between system automation trust and automation use as well as the theorized effect of the moderating variable of task load on this relationship. 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 briefly described the methods used to analyze the data collected during the experimental sessions.

IV.   Analysis Of Data

Data Analysis

      This chapter presents an analysis of the data (see appendix F) collected during the experiment described in Chapter III. The results of the information presented here, in relation to the research hypotheses, are presented in Chapter V. Correlation analysis was performed to statistically determine if relationships exit between perceptions of dependability, predictability and perceptions of trust in terms of system automation. In addition, correlation analysis was used to statistically determine if a relationship exists between perceptions of trust in automation and automation use. Finally, ANOVA was used to determine if user task load has a moderating effect on the relationship between system automation trust and use of system automation. Parametric statistical methods were used based on the assumption of normality of the data. The normality assumption is based on the graphical evidence presented in Figure 8 below. This figure presents two normal probability plots of the residual values (original value – estimate of the mean for each treatment group) from the initial and post-treatment trust questionnaire data. The straightness of the pattern in each of the plots provides strong support to the normality assumption (Devore, 2000). The parametric analysis methods used were: Pearson Correlations, Cronbach's Alpha, and ANOVA with a Tukey's multiple comparison. Cronbach's Alpha was used to evaluate the agreement in the perceived way the groups ranked the constructs in question.
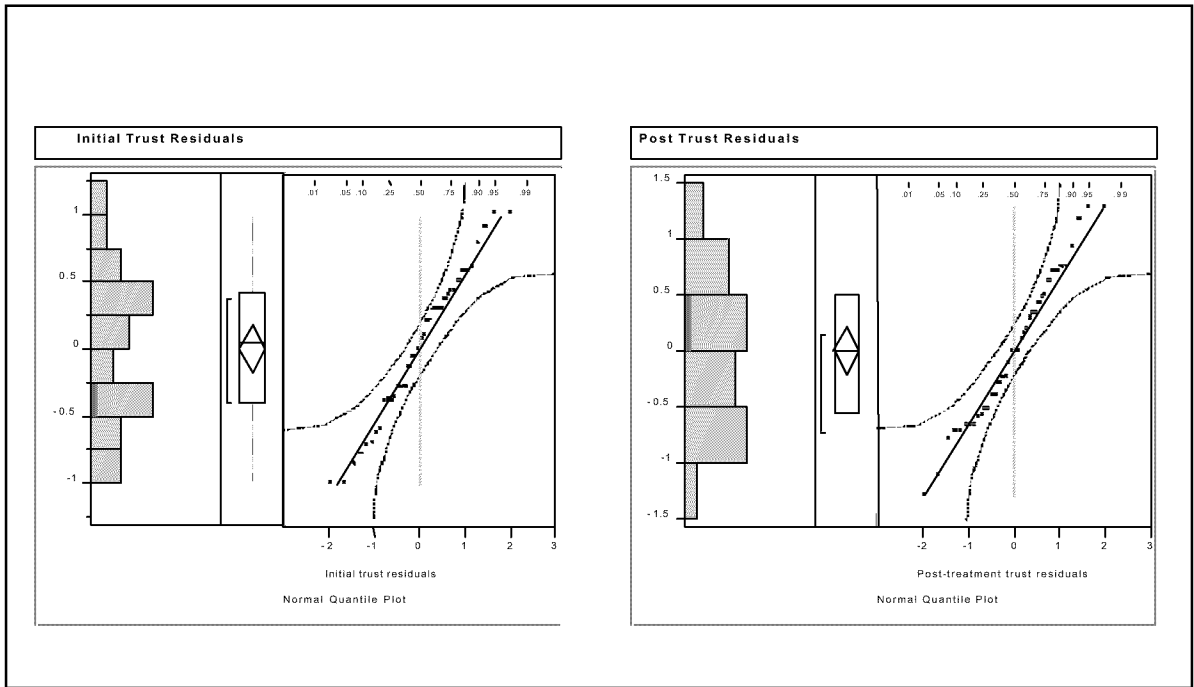
Figure 8: Normality Plots for Initial and Post-Treatment Trust Measure
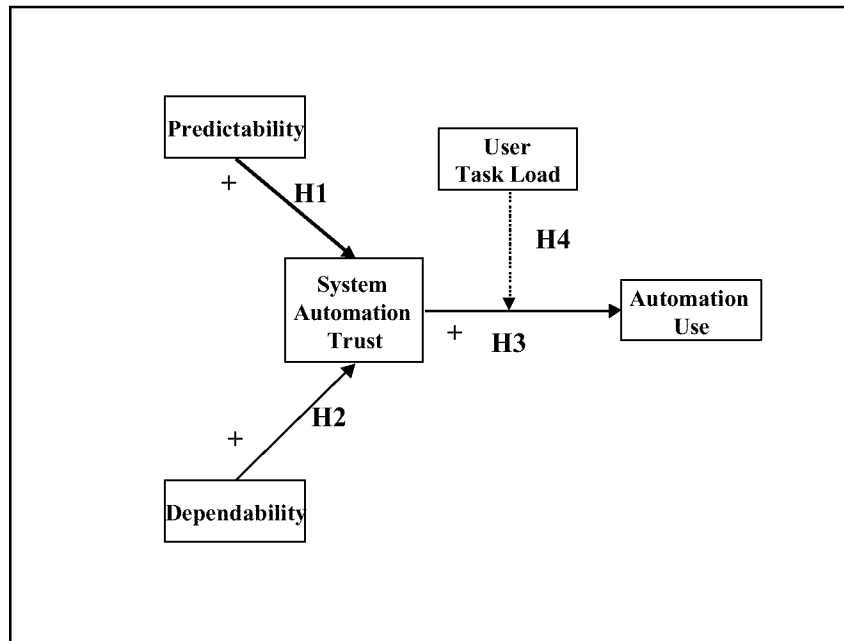
Figure 9: Developed Trust and Use Model

46

Relationship between predictability, dependability, and trust in system automation (H1, H2)

Hypothesis H1 predicts a positive correlation between perceptions of predictability of system automation with perceptions of trust in system automation, while hypothesis H2 predicts a positive correlation between perceptions of dependability of system automation with perceptions of trust in system automation. A review of the correlation analysis in Table 2 shows a statistically significant and strong positive correlation between perceived predictability and trust, and between perceived dependability and trust, both at a significance level of $\alpha < 0.01$. Values are shown for both pre-and post-treatment measures. Table 3 below presents a Cronbach's Alpha analysis and shows strong (alpha $> .7$) consistency of response in the measurements of trust and predictability (Sall et al., 2001). No Cronbach's analysis was accomplished for dependability due to the single question asked regarding this construct.

Table 2: Correlation Analysis for Predictability and Dependability vs. Trust

Constructs	Time Frame	Pearson Correlation r-value
Predictability	Pre-treatment	.4759
	Post-treatment	.6756
Dependability	Pre-treatment	.5734
	Post-treatment	.6878

Significant at p = .01

Table 3: Cronbach's Alpha Analysis

Construct	Time Frame	Cronbach's Alpha
Trust	Pre-treatment	.7967
	Post-treatment	.9244
Predictability	Pre-treatment	.7528
	Post-treatment	.7412
Entire Set	Pre-treatment	.8273
	Post-treatment	.9232

In addition to the Cronbach's Alpha analysis, a factor analysis was completed on the questionnaire data and verified two constructs were measured; trust and predictability, as was desired. The findings above support both Hypothesis 1 and 2 and suggest that as ratings of perceived predictability and dependability in system automation rise, so too, do ratings of trust in system automation.

Relationship between system automation trust and system automation use (H3)

Hypothesis 3 predicts that an individual's perception of trust in system automation will be positively correlated with his use of system automation. Automation use was measured as a ratio between the number of system recommendations given and the number of recommendations accepted by an individual. The higher the ratio, the greater the automation was used. A review of the correlation analysis presented in Figure 10 and Table 4 shows a statistically significant and strong positive correlation between ratings of trust in system automation and automation use at a significance level $\alpha < 0.01$ using post-treatment trust and automation measures. This finding supports Hypothesis 3 and suggests that as a user's perception of trust in system automation increases so will his use of that system's automation.

Table 4: Correlation Analysis for Trust vs. Automation Use

Construct	Pearson Correlation r-value
Trust Vs. Automation Use	.6839

Significant at p = .01
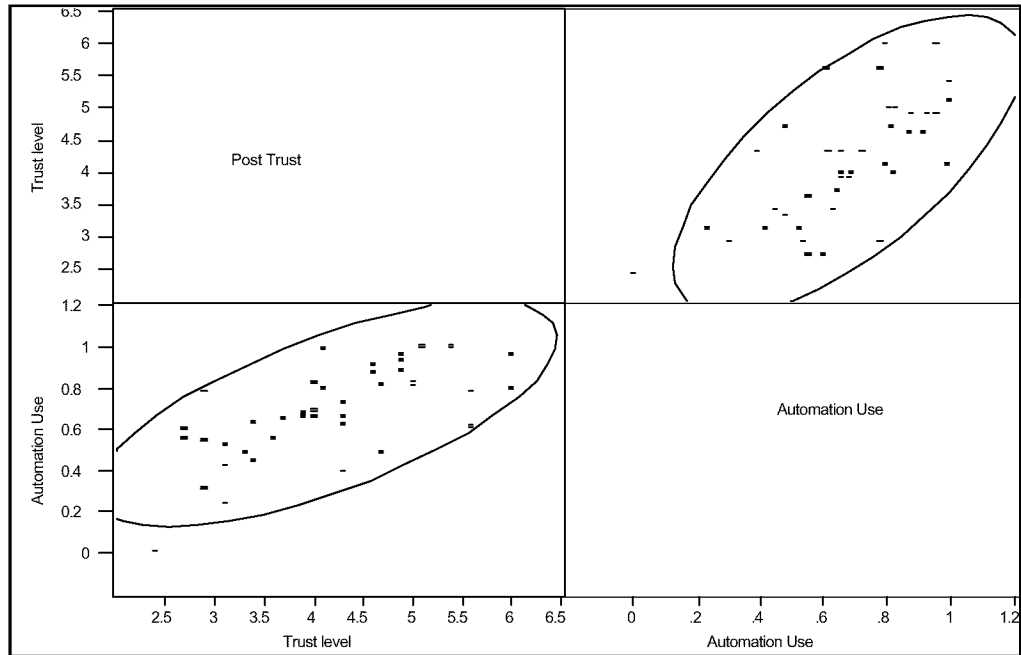
Figure 10: Scatter Plot of Trust vs. Automation Use

Moderating effect of user task load on the relationship between system automation trust and system automation use (H4)

Hypothesis 4 predicts a user's task load will have a moderating effect on the relationship between system trust and his use of system automation. The parametric results shown below in Figures 11, 12 and 13 provide evidence that task load has a moderating effect on the relationship between trust and automation use at a significant level of $\alpha < .05$. Figures 11 and 12 are ANOVA plots with associated Tukey's Multiple Comparison results showing the mean trust levels of each treatment group before and after treatments were applied. Figure 11 indicates all participants show a high level of system automation trust pre-treatment with no statistically significant difference between treatment groups.
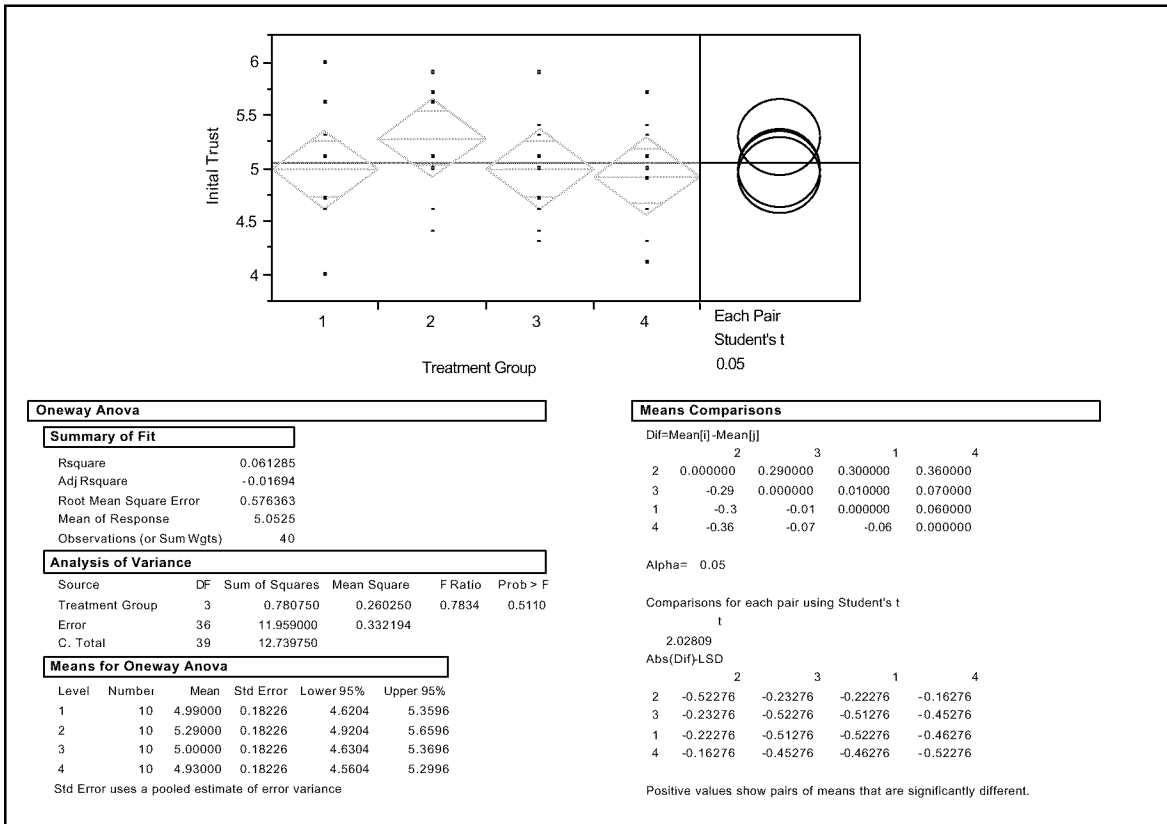
Figure 11: Descriptive Statistics of Pre-Treatment Trust Measures

However, the evidence shown in figure 12 below, does allow for the claim that treatments 1 and 3 are statistically significantly different from treatments 2 and 4 in their associated mean values of system automation trust. That is to say, the treatments in which information provided was not in question (i.e., non-IW) are significantly different from the treatments in which information was in question (i.e., IW) in terms of overall system automation trust.
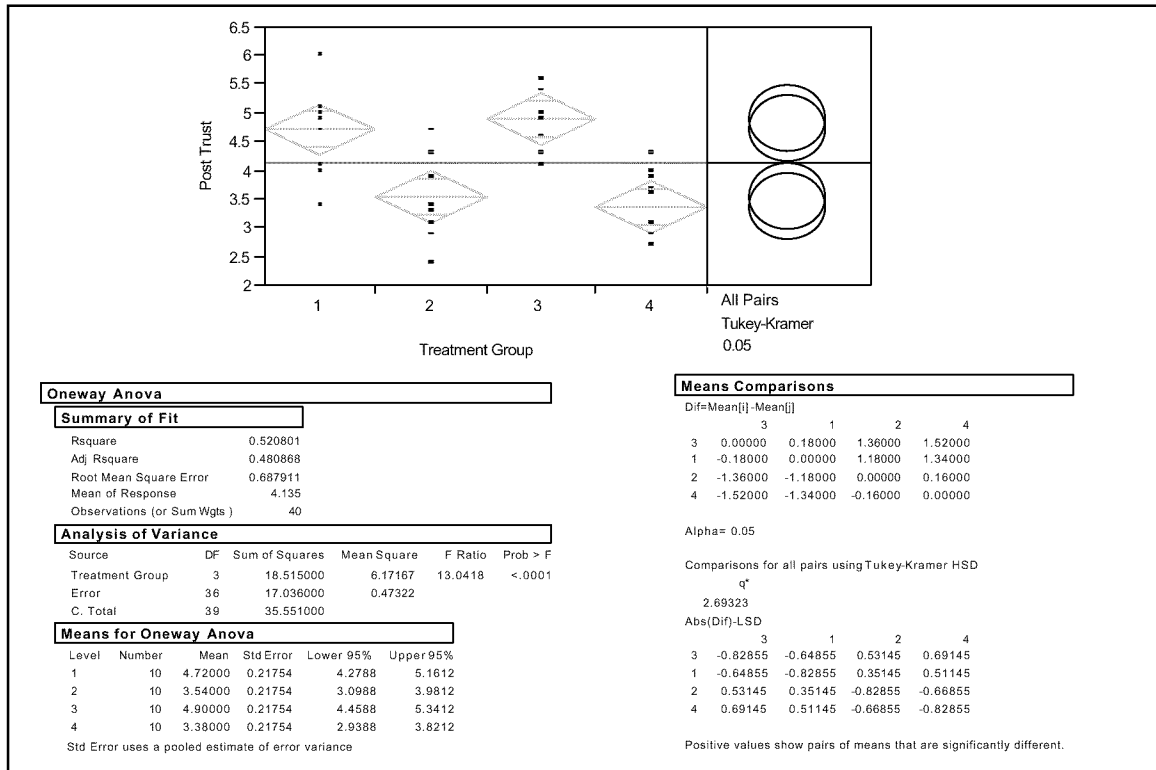
Figure 12: Descriptive Statistics of Post-Treatment Trust Measure

Oneway Anova

Summary of Fit

Rsquare	0.520801
Adj Rsquare	0.480868
Root Mean Square Error	0.687911
Mean of Response	4.135
Observations (or Sum Wgts)	40

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio	Prob > F
Treatment Group	3	18.515000	6.17167	13.0418	<.0001
Error	36	17.036000	0.47322		
C. Total	39	35.551000			

Means for Oneway Anova

Level	Number	Mean	Std Error	Lower 95%	Upper 95%
1	10	4.72000	0.21754	4.2788	5.1612
2	10	3.54000	0.21754	3.0988	3.9812
3	10	4.90000	0.21754	4.4588	5.3412
4	10	3.38000	0.21754	2.9388	3.8212

Std Error uses a pooled estimate of error variance

Means Comparisons

Dif=Mean[i]-Mean[j]

	3	1	2	4
3	0.00000	0.18000	1.36000	1.52000
1	-0.18000	0.00000	1.18000	1.34000
2	-1.36000	-1.18000	0.00000	0.16000
4	-1.52000	-1.34000	-0.16000	0.00000

Alpha= 0.05

Comparisons for all pairs using Tukey-Kramer HSD

q^*

2.69323

Abs(Dif)-LSD

	3	1	2	4
3	-0.82855	-0.64855	0.53145	0.69145
1	-0.64855	-0.82855	0.35145	0.51145
2	0.53145	0.35145	-0.82855	-0.66855
4	0.69145	0.51145	-0.66855	-0.82855

Positive values show pairs of means that are significantly different.

This information taken together with the results of hypothesis 3, which suggests that trust and automation use are positively correlated, could lead one to conclude that the levels of automation use between treatment groups 1 and 3 and between treatment groups 2 and 4 would show no statistically significant difference. Figure 12 below, shows that there is indeed no statistically significant difference in automation use between treatment groups 1 and 3, (high trust groups) but does show a statistically significant difference, although minor, between groups 2 and 4 (low trust groups). In should be noted that the confidence level for the entire set of comparison means is 95% (alpha of .05), but the confidence level for any particular comparison (i.e., treatment 2 and 4) is larger than 95% as the Tukey method uses an experiment-wise error rate rather than a pre-comparison error rate (Devore, 2000).
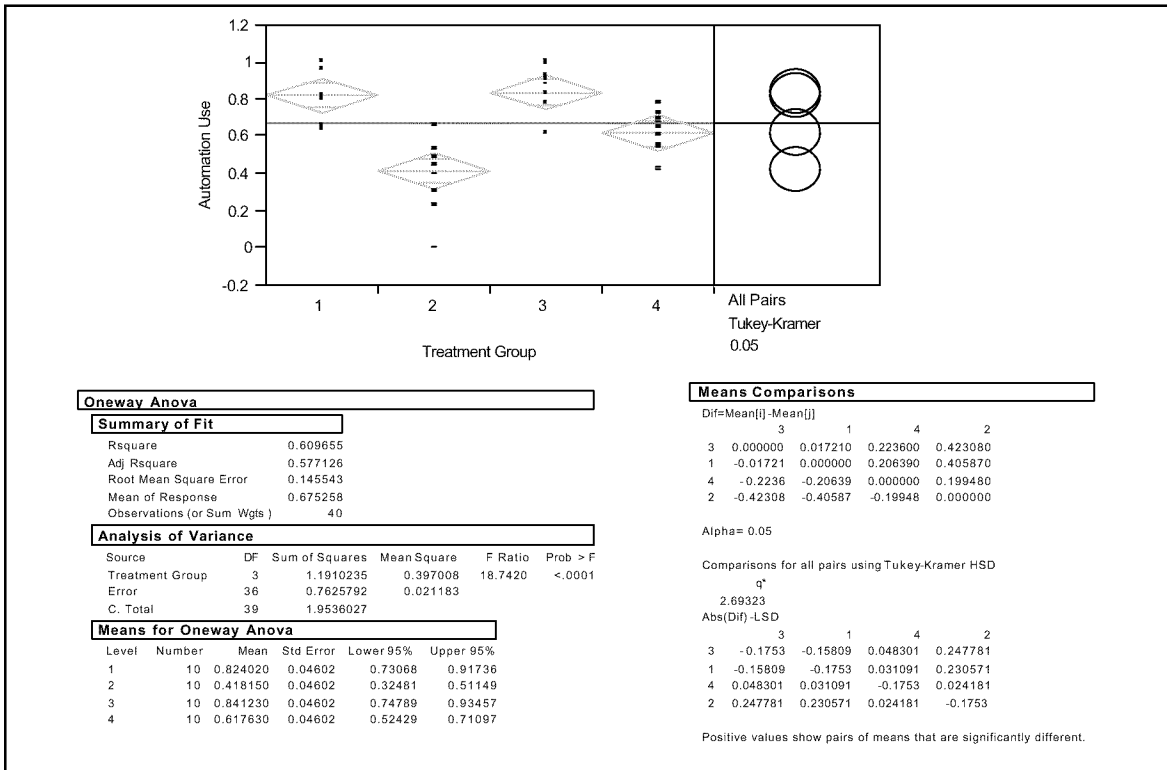
Figure 13: Descriptive Statistics of Post-Treatment Automation Use

Oneway Anova

Summary of Fit

Rsquare	0.609655
Adj Rsquare	0.577126
Root Mean Square Error	0.145543
Mean of Response	0.675258
Observations (or Sum Wgts)	40

Analysis of Variance

Source	DF	Sum of Squares	Mean Square	F Ratio	Prob > F
Treatment Group	3	1.1910235	0.397008	18.7420	<.0001
Error	36	0.7625792	0.021183		
C. Total	39	1.9536027			

Means for Oneway Anova

Level	Number	Mean	Std Error	Lower 95%	Upper 95%
1	10	0.824020	0.04602	0.73068	0.91736
2	10	0.418150	0.04602	0.32481	0.51149
3	10	0.841230	0.04602	0.74789	0.93457
4	10	0.617630	0.04602	0.52429	0.71097

Means Comparisons

Dif=Mean[i]-Mean[j]

	3	1	4	2
3	0.000000	0.017210	0.223600	0.423080
1	-0.01721	0.000000	0.206390	0.405870
4	-0.2236	-0.20639	0.000000	0.199480
2	-0.42308	-0.40587	-0.19948	0.000000

Alpha= 0.05

Comparisons for all pairs using Tukey-Kramer HSD

q*

2.69323

Abs(Dif)-LSD

	3	1	4	2
3	-0.1753	-0.15809	0.048301	0.247781
1	-0.15809	-0.1753	0.031091	0.230571
4	0.048301	0.031091	-0.1753	0.024181
2	0.247781	0.230571	0.024181	-0.1753

Positive values show pairs of means that are significantly different.

These findings support Hypothesis 4 and suggest that despite perceptions of low system automation trust, individuals tend to use automation more when task load s increased.

Conclusion

The findings from this chapter show some significant results and are discussed in the next chapter concerning the experimental hypotheses. In addition, Chapter V will provide an overview of the research findings, present some limitations associated with this research, discuss implications for the Air Force, and offer suggestions for follow-on research.

V.   Findings

Introduction

Automation in computer systems provides humans with a great deal of assistance in carrying out the responsibilities of our everyday lives. However, our willingness to use and trust this automation constrains its use. This research looked at the interactions between humans and computer automation and the effects the humans' perceptions of trust played in the way they utilized this automation. It also looked at how workload affected the relationship between trust and system automation use. This chapter examines the findings from the data analysis of the experiment described in Chapter III with respect to the research hypotheses offered in Chapter II. Next, implications for the Air Force are presented to include areas of further research. Finally, limitations of the research experiment are presented.

The research question for this study was to understand how an individual's trust in a computer system's automation affects his use of the system's automation and to examine what effects user task load has on his use of automation in an environment in which trust level is degraded; i.e., an IW environment. Four hypotheses were developed in Chapter II and tested in the experiment described in Chapter III. The conclusions of each of these research questions are presented below:

Perceptions of predictability and dependability of system automation will be positively correlated with ratings of trust (H1, H2)

Trust in computer automation, similar to human-human trust, is thought to be composed of many factors, two of which are predictability and dependability. This relationship was established in Muir and Morray's (1996) dynamic model of trust. As such,

predictability and dependability are hypothesized to be associated with trust of automation. This research showed that this appears to be the case. As ratings of predictability and dependability rise, so do ratings of trust. This relationship between predictability, dependability, and trust provide support for earlier work mentioned above by Muir and Morray (1996) indicating that predictability and dependability are components of trust. In addition, the results showed a slightly stronger correlation in both components in the post-treatment measures. This is in line with the notion that trust, even in human-machine relationships, is developed and strengthened over time. Results also support the notion that when an individual perceives unreliability in automation, his trust in that automation will decrease.

Trust in system automation will be positively correlated with use of system automation (H3)

Previous research in the use of technology and system automation found that an individual's use of a system's automation depended on his perceived reliability of the system, or trust in the system's automation (Zanna, 1985; Muir and Morray 1996). The results of this research add support to this notion as seen in the high positive correlation between perceived trust and system automation use. In the cases in which unreliability, in the form of indicated information warfare activities, was injected into the treatment scenarios, trust in the systems automation was significantly reduced. All individuals in the two treatment groups in which IW was indicated answered, "yes," to a post scenario question asking if the scenario indicated IW activities while no individuals in the non-IW treatment groups answered, "yes." This reduced level of trust resulted in a corresponding reduced level of automation use in these groups. This result, contrary to previous research (Fields, 2001), also suggests that

information warfare activities, by influencing the reliability of a system's performance, may result in lowering the trust an individual places in that system and thus, his subsequent use of the system's automation may be diluted. This condition may be desired, as over-trust in a system or system's functions during times of unreliability may result in an increased frequency of commission errors producing undesirable results.

User task load will have a moderating effect on the relationship between system automation trust and use of system automation (H4)

The analysis from the experiment provides support for the notion that task load has a moderating affect on the positive relationship between automation trust and automation use. In other words, in high task load situations, individuals were more prone to use system automation despite a lower level of system automation trust caused by unreliability in the system automation. This behavior is consistent with that found by Skitka, Mosier and Burdick (1996) and Wiekins (1994). In the low task load, unreliable information scenario, individuals had more time to maintain their situational awareness and make a more informed, deliberate decision using manual targeting methods. As task load was increased and the situation become more urgent, the completeness and accuracy of the individual's situational awareness may have decreased. This may have caused the individual to abandon the more complete and deliberate manual targeting technique favored by the low task load group in favor of the faster automated techniques in order to maintain a feel of control over the situation.

Research Finding Overview

As predicted, there is evidence to suggest the factors of perceived predictability and dependability in a system's automation are positively correlated with ratings of trust in the system's automation, and that this associated level of trust is positively correlated with the level of system automation use by an individual. Therefore, in order to encourage the use of system automation and provide the potential for decreased decision time for decision makers, system designers and developers must provide systems that provide a high level of system predictability and dependability.

There also appears to be evidence to suggest that task load may play an important role in modifying the level of use of system automation when trust in the automation is low, such as in conditions in which information warfare activities are or have been occurring. This finding may be significant in military settings in which commission errors caused by overuse of automation in unreliable situations may cause grave results.

Implications

Implications of findings are considered in two areas: research and application. In regards to research, the findings in this study are encouraging enough to continue this stream of research. As the overall size of the Air Force workforce decreases, automation may be used to offset the decrease in personnel and possibly put an increasing workload on the remaining individuals. It would be beneficial to determine a suitable range within which an individual can maintain an appropriate level of situational awareness so factors such as unreliability of system automation remain part of the decision maker's environmental cues used to make critical decisions. This suitable-range theory could be accomplished in future

research by varying the workload over time and seeing how the same individual reacts in the different reliability scenarios. Because this study dealt with inexperienced individuals in regards to weapons directors duties, it would be important to determine if these results hold true for actual weapons directors in a more realistic environment. Experience level and confidence in one's own abilities have been shown to affect the level of trust an individual places in a system and plays a role in the type and amount of automation an individual uses (Lee and Morray, 1994).

Past research has shown that trust is a dynamic construct and that once lost can be regained over time (Seong et al., 1998). Because environmental conditions can reduce the level of perceived system trust, and therefore, system automation use, further research is necessary in this area to investigate what actions can facilitate the regaining of an individuals trust in the system once perceived trust is reduced.

Applications of this research may be useful in developing offensive information warfare tactics. First, tactics could be developed to take advantage of the reduced level of perceived trust in a system caused by uncertainty of the environment. A perceived IW attack, whether actual or not, upon our adversary could force a decreased level of trust by their operators on their own system and its automation capabilities. This could increase their decision time, or OODA loop, and provide an increased advantage to our own decision makers. In addition, if through subterfuge, one is able to affect an adversaries system such that its automation capability provided erroneous results, the increased task load may cause a higher occurrence of automation commission errors by the adversary due to overuse of the unreliable system automation, at least until the erroneous results are discovered.

From a defensive standpoint, operational protocols could be developed such that in times of uncertainty, increasing personnel to limit the effects of over-use of system automation could reduce individual workload. Also, it may be possible to maintain an individual's situational awareness regarding uncertainty in a system's performance by providing on-screen indications of the uncertainty and system reliability. These cues may help reduce the amount of automation use by individuals and thus, fewer commission errors would be committed.

Research Limitations

Despite the evidence in support of these results, certain limitations must be acknowledged when considering these findings. First, in regards to design and internal validity issues, repeated testing and instrumentation may be a threat to the internal validity. The same trust measurement questionnaire was given immediately before and immediately after the treatment scenario. This may have led at least some of the to answer trust questions based on their previous answers realizing that this was a test measure and they wanted to be consistent.

In consideration of external validity and generalizability issues, the population, military culture, and education level in which experiment subjects were drawn from may not be representative of the larger overall military population and even less representative of the civilian population. All but one of the experiment participants indicated they liked using computers for work and 90% indicated they felt comfortable with the role of computers in the Air Force. The setting in which the experiment was conducted may also lesson the external validity of this experiment. The somewhat sterile and unrealistic laboratory setting may have detracted from the desire to instill a command and control atmosphere and may

have resulted in less effective manipulations. In addition, due to equipment limitations, there was no way for actual manipulation of the software to mimic realistic IW activities. Despite, meeting the minimal AWDT vendor system specifications, the computers used were not powerful enough to run in a client-server mode as originally desired. This mode would have allowed real-time information manipulation during the treatment scenario. Also, subjects had no experience with the typical duties of an AWACS weapons director. Therefore, their experience level in this unique command and control environment was solely provided by the training they received during the experiment. Lack of experience may have contributed to a higher level of trust and subsequent automation use in the two treatment groups in which information provided was said to be reliable.

In regards to the trust measurement instrument used bias may have been introduced into the questionnaire due to the sequential nature of the questions. The first seven questions dealt with trust, the next three dealt with predictability, and the last dealt with dependability. In the future, if a similar questionnaire is used, questions should be reordered such that constructs are not measured in a sequential manner but rather in a random fashion.

Last, despite the strong support for normality, the analyses suffered from a small sample size and thus a lack of power to detect small effects. This is not an uncommon consequence of this type of field research due to cost and time in securing larger sample sizes from a border population. However, this does make significant findings more valuable when considering the implications. In addition, because this research is making claims against theory rather than generalizations to a larger population, the small sample size is not as significant a factor.

Summary

There appears to be evidence to suggest an individual's use of a system's automation capability is directly and positively related to the level of perceived trust the individual places in that system's automation. In addition, an individual's task load may have a moderating affect on the relationship between user trust and automation such that, during times of increased task load, an individual may resort to using the system automation despite a lower level of perceived trust in the system's automation. These results have important implications for the United States Air Force in that overuse of our automation capabilities by individuals may cause the increased occurrence of automation commission errors causing undesired and possibly catastrophic effects. In addition, the results indicate possible benefits in the area of offensive information warfare tactics. If tactics can be developed and implemented upon our adversaries to take advantage of the effects caused by a decreased level of trust in system automation and the overuse caused by increased workload, we could see an increase in an adversary's OODA loop and an increase in their commission of automation commission errors. Further research is warranted and should draw upon the results presented here while improving upon the mentioned limitations.

Appendices

Appendix A: Participant Information Sheet

<u>**Participant Information Sheet**</u> **(Form 2)**   **Participant ID#** _____

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. Service (USAF, Army, Navy) _____
4. AFSC _____
5. Are you currently in ROTC _____
6. Number of years served in current AFSC _____
7. Total number of years served in the military _____
8. Highest Level of Education (circle one): High School, Undergraduate, Graduate, Doctoral
9. Operational experience in Combat/Hostile Duty Location (yes/no) _____

SECTION II – Computer Experience an Attitudes (Circle One)

1. Are you currently, or have you ever, worked in a computer communications position? Y N
2. Do you consider yourself to be knowledgeable about computers?   Y N
3. Are you familiar with how a computer network operates?   Y N
4. Are you familiar with any programming languages?   Y N
5. Which computer programs do you use on a frequent basis
    _____
6. Do you like to use computers to conduct work?   Y N
7. Do you feel comfortable with the role computers play in today's Air Force?   Y   N
    Why or why not?

    _____

    _____

Appendix B: Automation Trust Survey

Participant Questionnaire   (Form 3)   Participant ID _____

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

1 = Disagree Very Strongly   2 = Disagree Strongly   3 =

Disagree

4 = Agree   5 = Agree Strongly   6 = Agree Very Strongly

1. ___I trusted the agent's recommendations

2. ___I was cautious in relying on the agent's recommendations

3. ___The agent influenced my decisions

4. ___I was willing to accept the agent's recommendations during risky situations in the scenario

5. ___I was willing to accept agent recommendations during non-risky situations in the scenario

6. ___I would trust the agent to perform certain tasks on my behalf

7. ___I was willing to accept the agent's recommendations during uncertain situations in the scenario

8. ___The agent's recommendations were predictable

9. ___The agent provided consistent information

10. ___The agent responded consistently to similar circumstances at different points in time

11. ___The agent was dependable

Appendix C: Sample Scenario Brief

BACKGROUND:

You are a Weapons Director aboard an E-3 AWACS aircraft from the 960th Airborne Air Control Squadron recently deployed to the Mediterranean Sea in support of operation Enduring Freedom. Your aircraft has just arrived on station at 33,000 ft, just west of the Island country of Malta. You have complete communications capabilities with all U.S. and allied aircraft and ground units in the current area of operation, which includes all of the Mediterranean Sea around the islands of Gozo and Malta.

THE PRESENT: Prior to takeoff, you received a crew briefing which included a standard Mission briefing, Intelligence briefing, and the current Rules of Engagement briefing. The following is a summary of the information you received.

MISSION:

Primary - Defend your assigned area of operation against any hostile enemy aircraft.

Secondary - Attack enemy airbases and resources as friendly resources allow.

INTEL BRIEF:

In response to the September 11th, 2001 terrorist attacks on the United States, the President, in coordination with the allied coalition has ordered the deployment of U.S. troops to areas around the world to include the Mediterranean Sea. In particular, U.S. Forces have been deployed, by invitation, to the island nation of Malta as a staging area for possible future military action in the war against terrorism.

Due to the American and coalition campaign against the Taliban regime in Afghanistan, Usama Bin Laden has called out to the Muslim world for a "Jihad" or "holy war" against the U.S and those adding us in our so called "quest for domination of the Muslim World."

In response to this call, Islamic extremists based in Algeria, just south of Malta, along with skilled members of the Al Qaeda terrorist network have overrun the Algerian backed country of Gozo and have seized control of all their military assets.

It is believed the extremists will attempt to use the Gozo air bases and aircraft for an all out suicide attack against American resources and American occupied airbases in the country of Malta. It is known that the Gozo military assets include Russian-made fighters, bombers, tankers as well as surface-to-air missile batteries.

Members of the Al Qaeda terrorist network are believed to be well trained in the art of information warfare. The CIA indicates many have been trained by the Peoples Republic of China's Information Warfare Force (IWF) and that the IWF has, in the past, sold some of its advanced electronic hacking equipment to the Al Qaeda.

EQUIPMENT STATUS: All systems up and running. Weapons Director system was down for a short time but is now back on line. It appears there has been an information warfare

attack on the system through the data and sensor uplink protocol. All indications are that

graphical display send and receive algorithms are working correctly. The algorithms that

affect the agent tool recommendations seem to have been the target of the attack. System

testing has shown an approximate 15% decrease in the effectiveness and reliability of the

recommendations.

Problem is being worked.

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

Malta airspace and to execute offensive strikes against all military capable targets on the

island of Gozo.

Appendix D: Sample Scenario Brief

BACKGROUND:

You are a Weapons Director aboard an E-3 AWACS aircraft from the 960th Airborne Air Control Squadron recently deployed to the Mediterranean Sea in support of operation Enduring Freedom. Your aircraft has just arrived on station at 33,000 ft, just west of the Island country of Malta. You have complete communications capabilities with all U.S. and allied aircraft and ground units in the current area of operation, which includes all of the Mediterranean Sea around the islands of Gozo and Malta.

THE PRESENT: Prior to takeoff, you received a crew briefing which included a standard Mission briefing, Intelligence briefing, and the current Rules of Engagement briefing. The following is a summary of the information you received.

MISSION:

Primary - Defend your assigned area of operation against any hostile enemy aircraft.

Secondary - Attack enemy airbases and resources as friendly resources allow.

INTEL BRIEF:

In response to the September 11th, 2001 terrorist attacks on the United States, the President, in coordination with the allied coalition has ordered the deployment of U.S. troops to areas around the world to include the Mediterranean Sea. In particular, U.S. Forces have been deployed, by invitation, to the island nation of Malta as a staggering area for possible future military action in the war against terrorism.

Due to the American and coalition campaign against the Taliban regime in Afghanistan, Usama Bin Laden has called out to the Muslim world for a "Jihad" or "holy war" against the U.S and those adding us in our so called "quest for domination of the Muslim World."

In response to this call, Islamic extremists based in Algeria, just south of Malta, along with skilled members of the Al Qaeda terrorist network have overrun the Algerian backed country of Gozo and have seized control of all their military assets.

It is believed the extremists will attempt to use the Gozo air bases and aircraft for an all out suicide attack against American resources and American occupied airbases in the country of Malta. It is known that the Gozo military assets include Russian-made fighters, bombers, tankers as well as surface-to-air missile batteries.

EQUIPMENT STATUS: All systems up and running.

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 Malta airspace and to execute offensive strikes against all military capable targets on the island of Gozo.

Appendix E: Post Simulation Evaluation Sheet

Post Simulation Evaluation Sheet (Form 5)   Participant # _____

INSTRUCTIONS

This is a short survey to assess the participant's reaction to the simulation. Please circle the correct answer.

1. Were the instructions clear and understandable?   Y   N

2. Was the simulation easy to understand?   Y   N

3. Was the training sufficient for you to play the game?   Y   N

4. Did you encounter any difficulties in following the instructions for the game?   Y   N

5. Was the game's operations tempo too fast?   Y   N

6. What did you perceive the workload as: High or Low

7. Was Information Warfare activity indicated in your scenario?   Y   N

Thank you for participating in this research. Your inputs are extremely valuable.

Appendix F: Compiled Data

Task Load/ Reliability	Treatment Group	Initial Trust	Initial Predictability	Initial Dependability	Post Trust	Post Predictability	Post Dependability	% Automation Use	Average Load	Pre- Treatment Trust Residuals	Post- Treatment Trust Residuals
Low Non Information Warfare	1	5.6	5.3	6.0	6.0	4.0	3.0	0.80	0.20	0.6	1.28
	1	4.6	6.0	6.0	4.7	5.7	6.0	0.81	0.08	-0.4	-0.01
	1	4.0	3.7	4.0	4.0	4.0	4.0	0.82	0.06	-1.0	-0.72
	1	4.0	4.0	4.0	4.1	4.0	4.0	0.79	0.08	-1.0	-0.58
	1	4.7	5.0	5.0	3.4	3.0	4.0	0.63	0.08	-0.3	-1.29
	1	5.1	5.0	5.0	4.9	4.0	4.0	0.95	0.07	0.2	0.14
	1	6.0	5.7	6.0	4.0	4.7	3.0	0.66	0.06	1.0	-0.72
	1	4.6	4.7	5.0	5.0	4.7	5.0	0.81	0.08	-0.4	0.28
	1	6.0	5.7	6.0	5.1	4.0	6.0	1.00	0.07	1.0	0.42
	1	5.3	5.3	6.0	6.0	5.0	6.0	0.96	0.03	0.3	1.28
Low Information Warfare	2	5.7	5.3	5.0	3.1	3.3	3.0	0.23	0.09	0.42	-0.40
	2	5.6	6.0	5.0	2.9	3.3	3.0	0.30	0.16	0.28	-0.68
	2	5.1	5.3	4.0	4.3	4.7	3.0	0.66	0.06	-0.15	0.75
	2	5.0	4.3	4.0	4.7	4.0	4.0	0.48	0.10	-0.29	1.17
	2	4.6	4.3	4.0	3.1	4.0	2.0	0.53	0.09	-0.72	-0.40
	2	5.9	5.3	6.0	3.4	4.0	3.0	0.44	0.10	0.57	-0.11
	2	5.9	5.7	6.0	2.4	2.7	3.0	0.00	0.10	0.57	-1.11
	2	5.7	5.0	5.0	3.9	3.7	4.0	0.66	0.05	0.42	0.32
	2	5.0	4.7	5.0	3.3	4.0	4.0	0.48	0.15	-0.29	-0.25
	2	4.4	5.0	5.0	4.3	3.7	4.0	0.39	0.08	-0.86	0.75
High Non Information Warfare	3	4.4	4.3	4.0	4.9	4.3	5.0	0.93	0.20	-0.6	0.0
	3	5.4	4.7	6.0	4.6	4.3	5.0	0.91	0.29	0.4	-0.3
	3	5.9	5.7	6.0	5.4	4.7	5.0	1.00	0.26	0.9	0.5
	3	5.0	4.7	5.0	5.6	4.7	5.0	0.61	0.20	0.0	0.7
	3	5.3	4.3	5.0	4.9	4.3	6.0	0.88	0.17	0.3	0.0
	3	5.1	3.7	5.0	4.1	4.0	4.0	0.99	0.25	0.1	-0.8
	3	4.6	4.7	6.0	5.0	4.0	5.0	0.83	0.27	-0.4	0.1
	3	4.3	5.0	4.0	4.3	4.7	4.0	0.61	0.31	-0.7	-0.6
	3	4.7	4.3	4.0	4.6	3.7	4.0	0.87	0.34	-0.3	-0.3
	3	5.3	4.3	5.0	5.6	4.7	5.0	0.78	0.34	0.3	0.7
High Information Warfare	4	4.3	5.0	5.0	3.1	2.3	3.0	0.42	0.32	-0.64	-0.24
	4	4.6	5.0	5.0	4.0	3.0	3.0	0.69	0.32	-0.36	0.62
	4	4.9	4.7	5.0	2.7	3.0	3.0	0.55	0.36	-0.07	-0.67
	4	4.1	4.3	4.0	2.9	3.3	4.0	0.54	0.33	-0.79	-0.52
	4	5.7	4.0	4.0	3.6	3.3	4.0	0.55	0.39	0.78	0.19
	4	5.4	6.0	6.0	3.9	3.7	3.0	0.68	0.32	0.50	0.48
	4	5.0	4.0	5.0	2.7	3.0	2.0	0.60	0.30	0.07	-0.67
	4	5.1	4.0	4.0	2.9	3.7	3.0	0.78	0.37	0.21	-0.52
	4	4.9	5.0	5.0	3.7	3.3	4.0	0.65	0.21	-0.07	0.33
	4	5.3	4.3	5.0	4.3	2.7	3.0	0.72	0.27	0.36	0.91

Appendix G: Participant Treatment-Group Assignment

Randomized Block Design			
Participant ID	Reliability Treatment Group	Task Load	Weapons Director Position
1	Non-IW	Low	1
2	Non-IW	Low	2
3	Non-IW	Low	3
4	Non-IW	High	1
5	Non-IW	High	2
6	Non-IW	High	3
7	IW	Low	1
8	IW	Low	2
9	IW	Low	3
10	IW	High	1
11	IW	High	2
12	IW	High	3
13	Non-IW	Low	1
14	Non-IW	Low	2
15	Non-IW	Low	3
16	Non-IW	High	1
17	Non-IW	High	2
18	Non-IW	High	3
19	IW	Low	1
20	IW	Low	2
21	IW	Low	3
22	IW	High	1
23	IW	High	2
24	IW	High	3
25	Non-IW	Low	1
26	Non-IW	Low	2
27	Non-IW	Low	3
28	Non-IW	High	1
29	Non-IW	High	2
30	Non-IW	High	3
31	IW	Low	1
32*	IW	Low	2
33*	IW	Low	3
34	IW	High	1
35*	IW	High	2
36*	IW	High	3
37*	Non-IW	Low	1
38*	Non-IW	High	2
39*	IW	Low	3
40	IW	High	1

* Indicates ROTC Student

Why Are You Here

- To help in early field trials of emerging software technology that will aid Weapons Directors aboard E-3 AWACS Aircraft
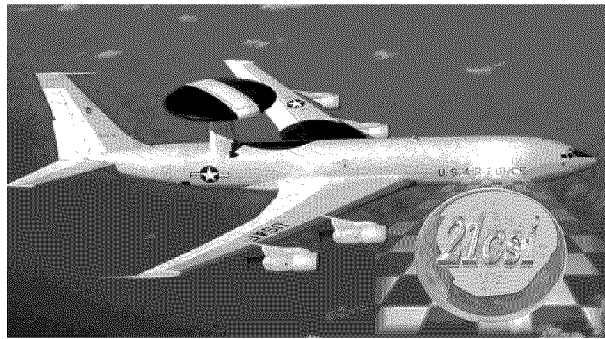
1

Schedule of Events
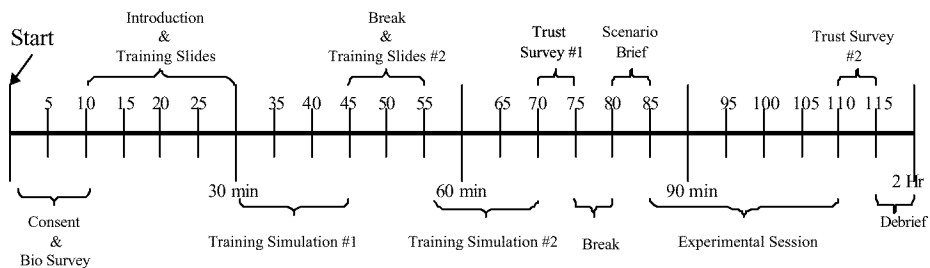
2

Agent-based Command, Control and Communications for AWACS Weapons Director Teams
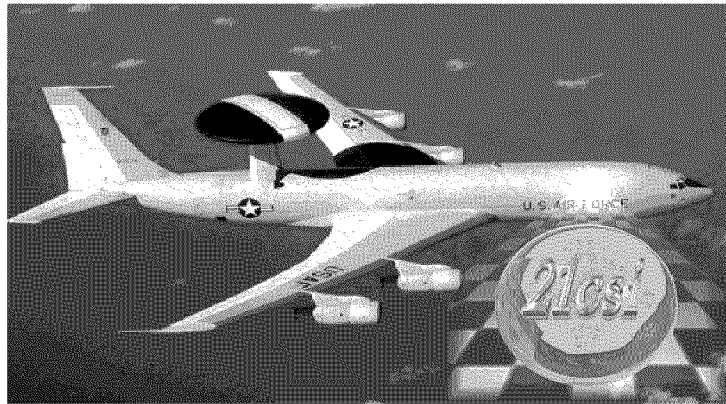
1/21/2002

5

Top Control Panel

Mission
Information

Activate
Help
Agent

Measures
Selector

AF-DCA   Standard Map

Player
Selector

Auto-Accept
Mode

Agent
Enabler

SAM
Avoidance
Agent

Display the
Director's Lane

Accept
All
Recommendations

6

Controls

AF-DCA   Standard Map

Player
selector

Agent
enabler

Accept all
recommendations

Mission
information

Display the
Director's Lane

Activate the
Help Agent

Measures
selector

7

73

Some System Functions

- **Logging In** (All you need to enter is your participant ID)

- **View Mission Information**

- **Viewing Events**

- **Zooming**

- **Panning**

- **Viewing Scores**

8

System Functions (Continued)

- **Automatic accepting of Recommendations**

- **Manual accepting of Recommendations**

9

Logging In (Result)
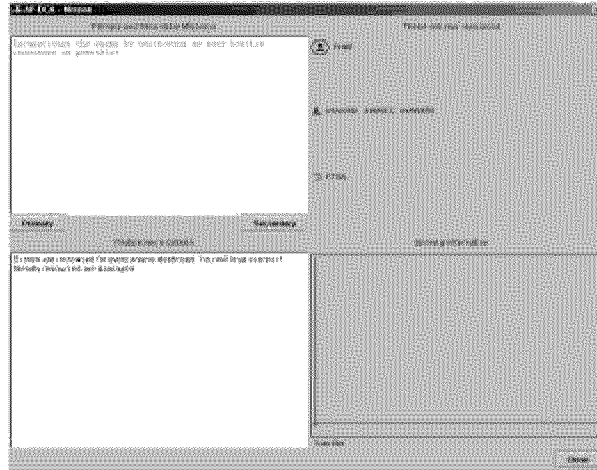
10

Viewing mission information

* **Click Mission Information Button**

* **View Mission Information Window**

11

Click Mission Information Button
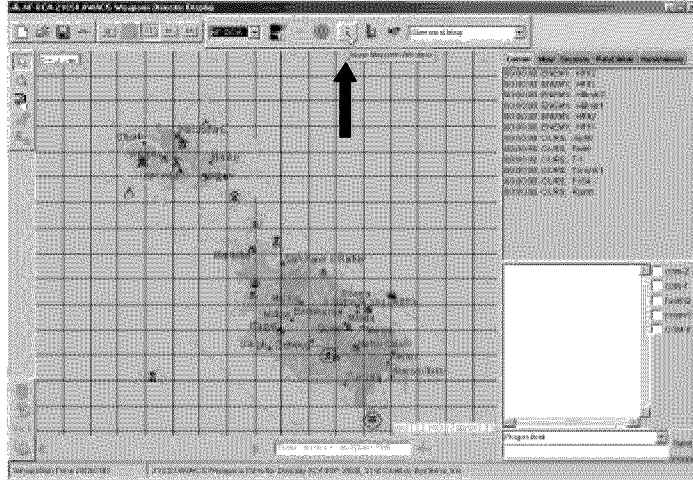
12

View Mission Information Window
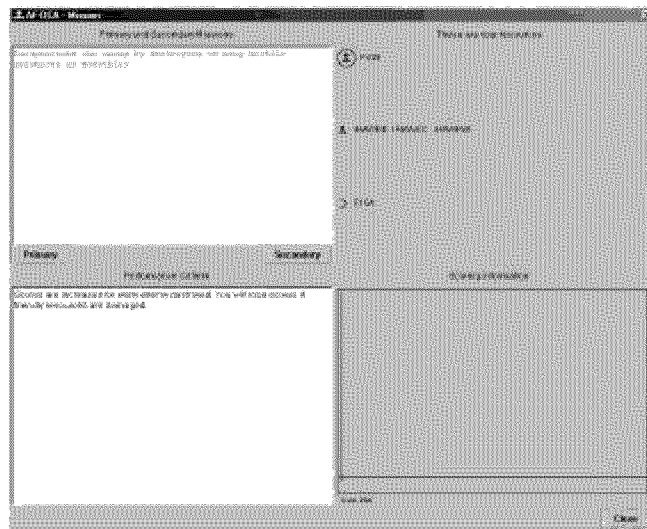
13

Viewing Events

- **Make sure the Communication Panel is displayed.**

- **View the Events**

14

Display Communication Panel

15

View the Events

16

Zooming

- **Make sure the Navigation Panel is displayed**

- **Select desired zoom ratio**

17
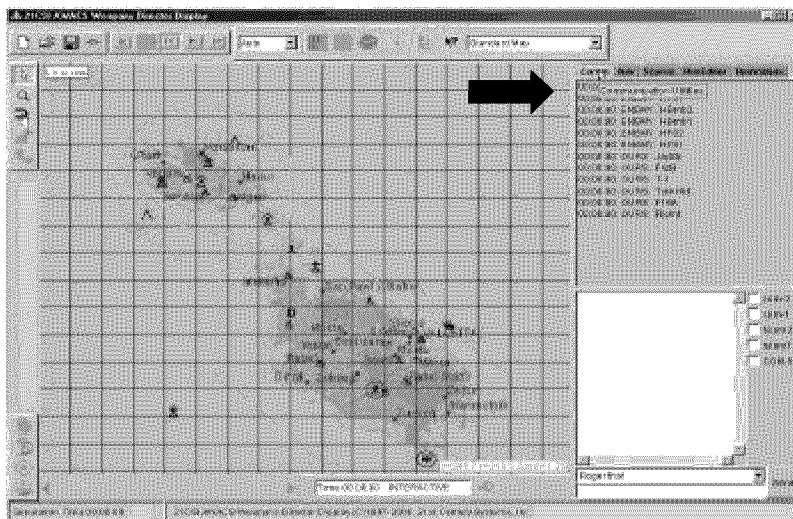
Display Navigation Panel
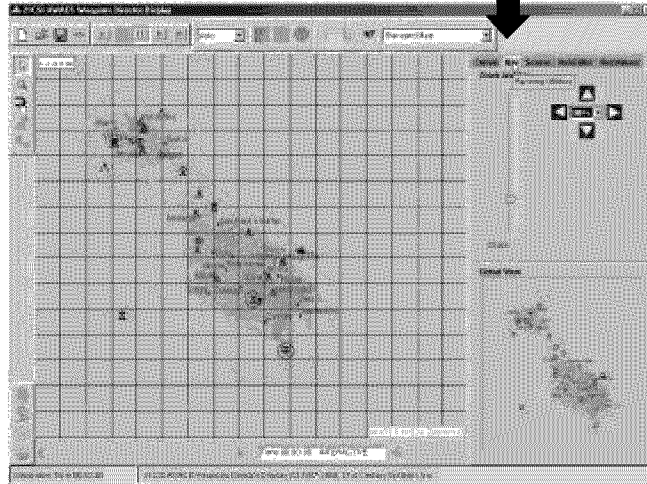
18

Select desired zoom ratio

19
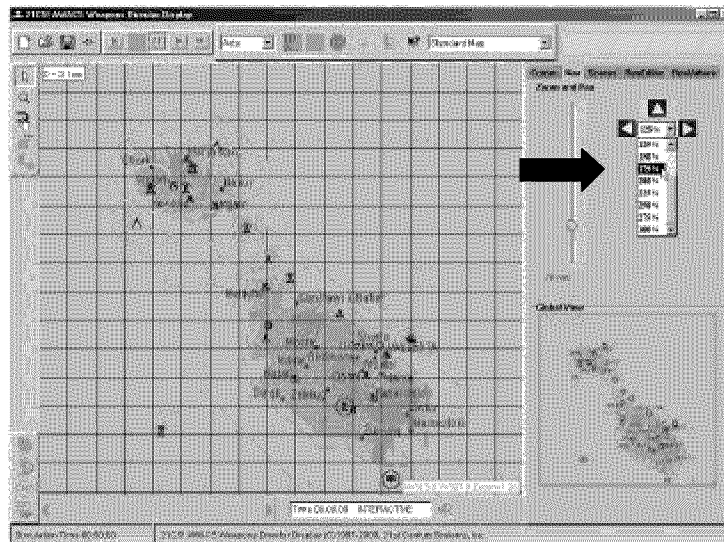
ZOOM Result
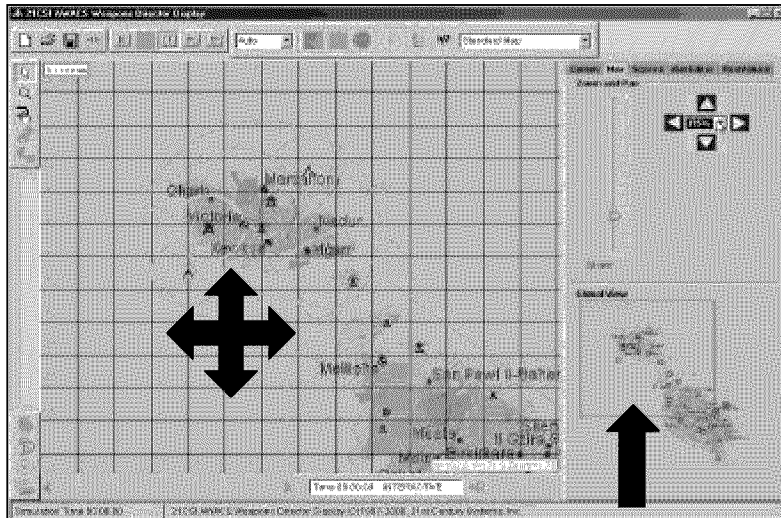
Panning

- **Make sure the Navigation Panel is displayed**

- **Press the map in the desired direction**

Display Navigation Panel
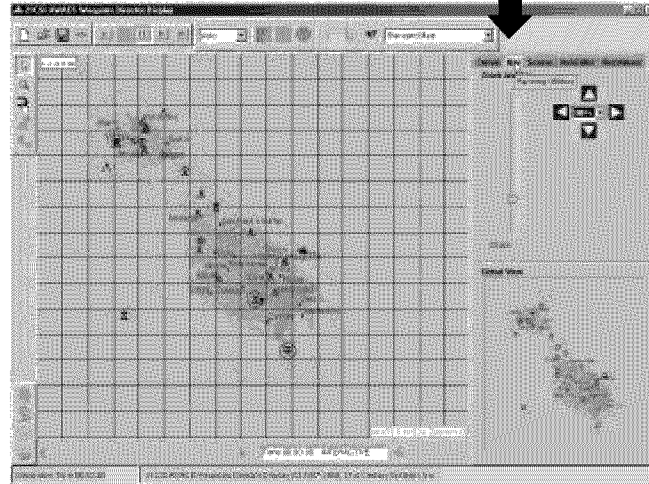
22

Press the map in desired direction
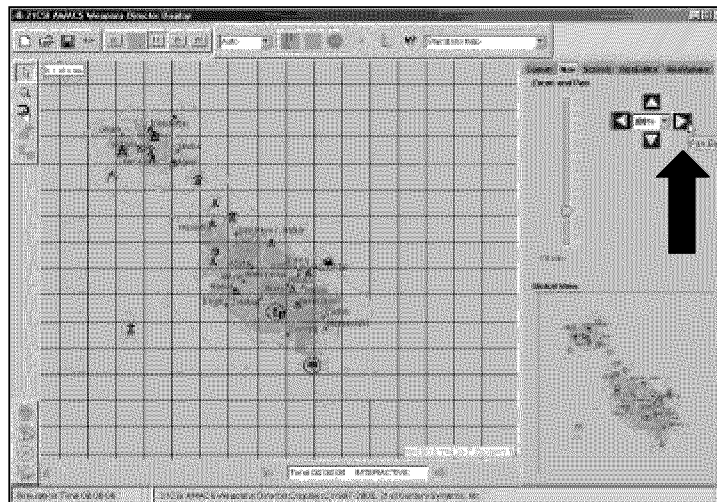
23

PAN Result
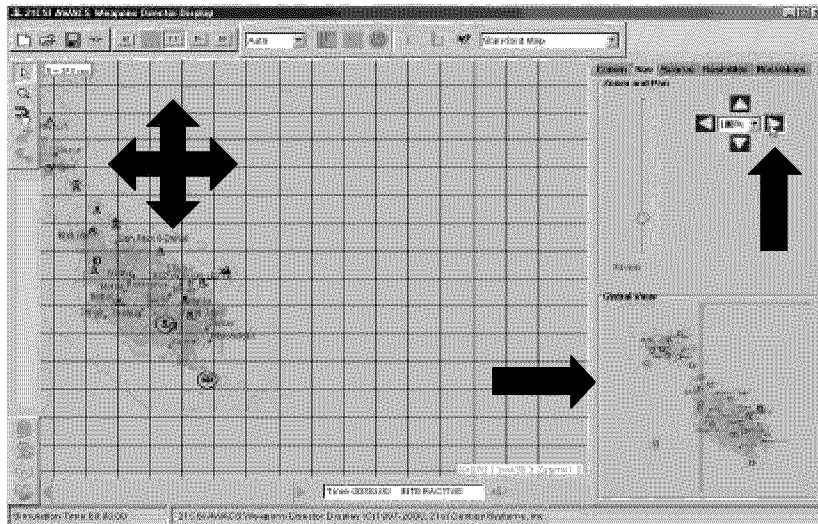
24

Mode Dependent Functions

→ Standard Mode

→ Zoom In/ Zoom Out

→ Special Mode
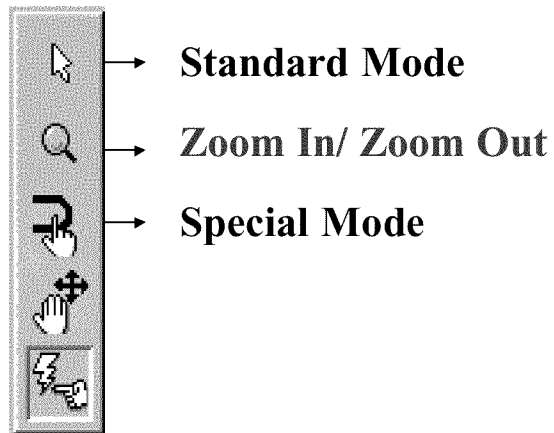
26

Standard Mode

• Issue Orders

• **View a Resource's Information**

• Manually accept a single recommendation (will cover this later)

27

To Issue Orders You:

• **Left click on the resource you wish to issue an order to.**
• **Right click on desired target resources.**
• **Right click on the map for GO orders.**
• **Left click on the map to process the orders.**

28

Left click on the resource you wish to issue an order to
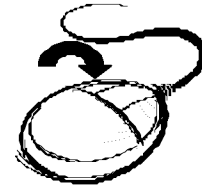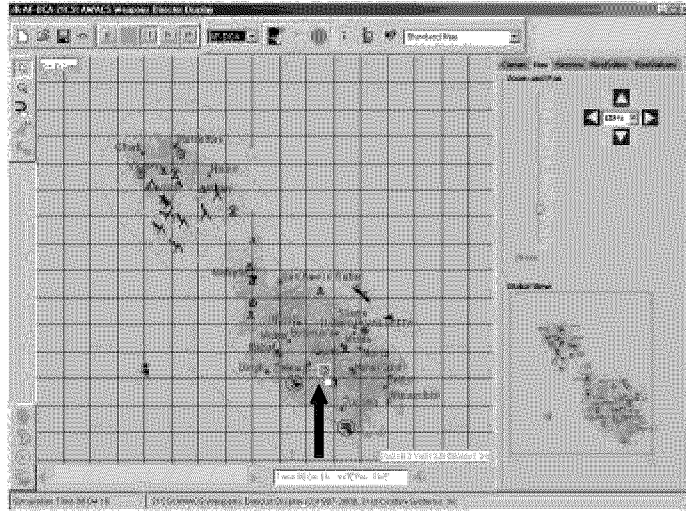
29

Right click on desired target resources
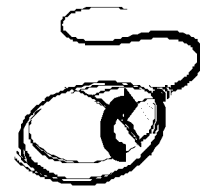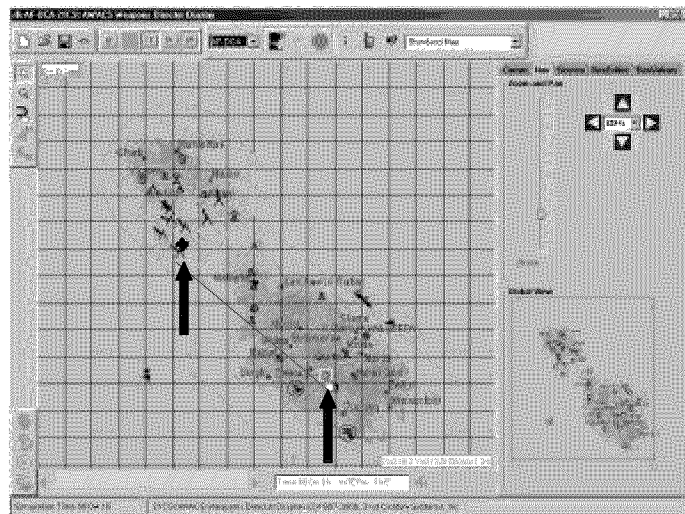
30

Right click on the map for GO orders
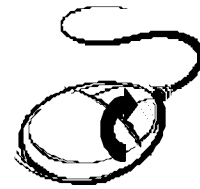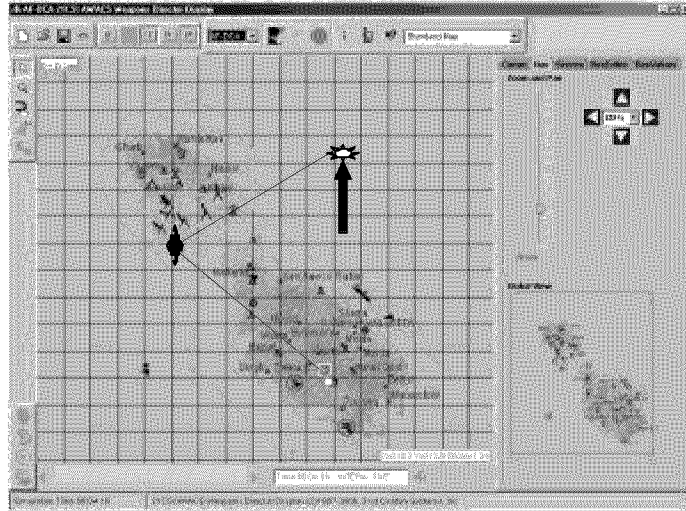
31

Left click on the map to process the orders
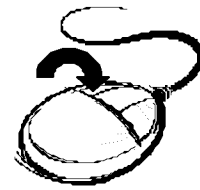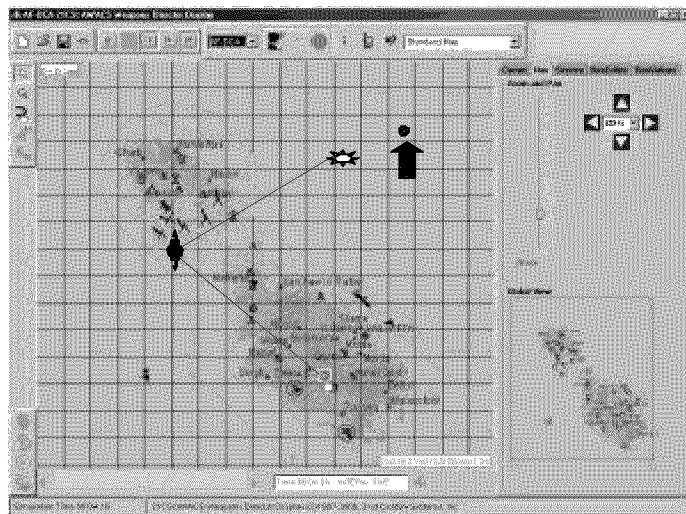
32

View a resource's information

- **Right click on the desired resource to display an information window**

- **Click on the information window to close it**

33

Right click on resource for information window
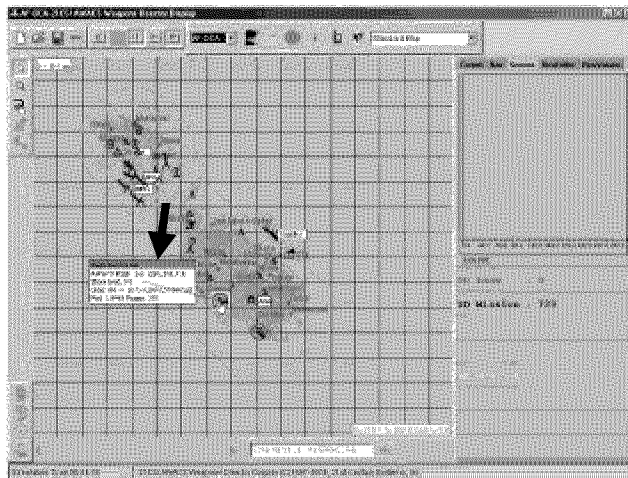
34

Left click on the information window to close it
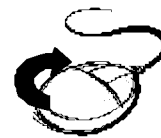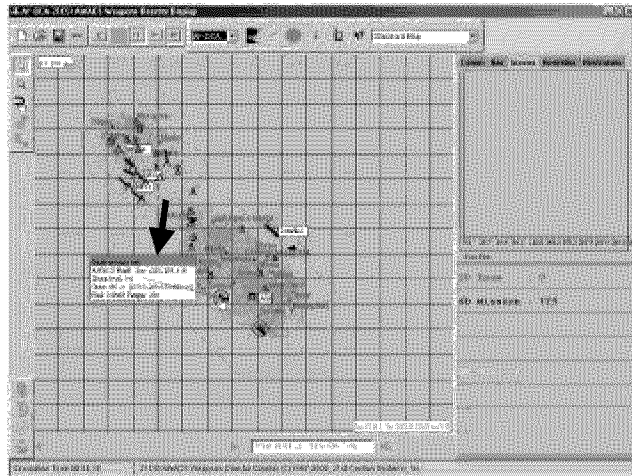
35

Zoom Mode

- **Zoom In**
  - Left click on the map

- **Zoom Out**
  - Right click on the map
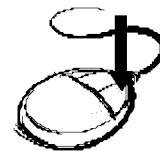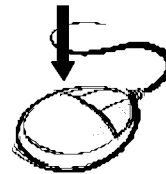
36

Special Mode

• **Display Properties**

37

Properties' display
Left click on the map
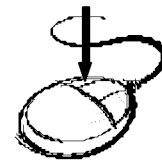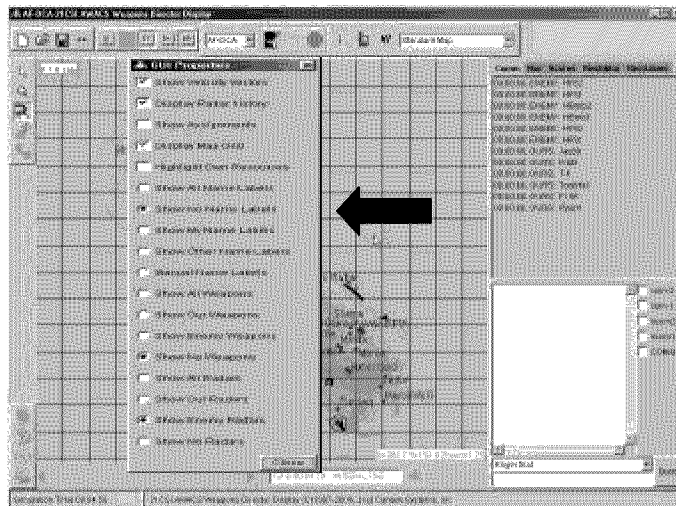
38

Interceptor

Friendly   **Hostile**

Not Paired

Paired
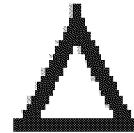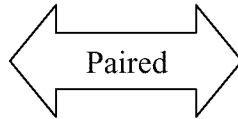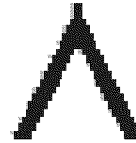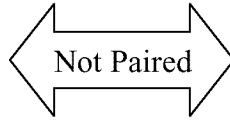
39

Bomber and General Air

Friendly   **Hostile**

Not Paired

Paired
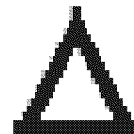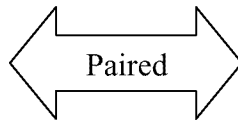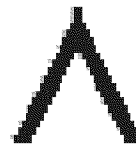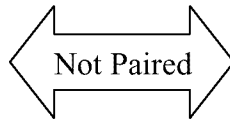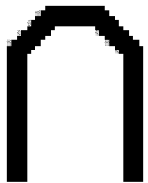
40

AWACS/Hawkeye

Friendly

Not Paired

Paired

41

JSTARS/RJ

Friendly

Not Paired

Paired

42

90

Tanker

Friendly

Not Paired

Paired
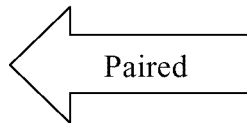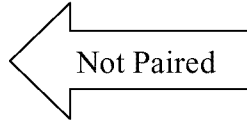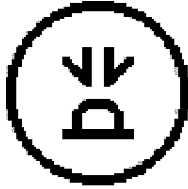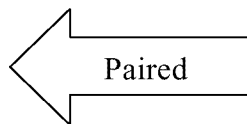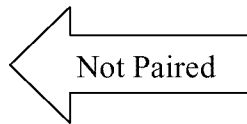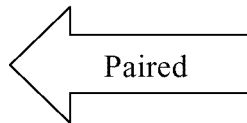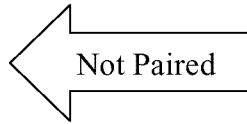
43

Jammer
Special Mission

Friendly

Not Paired

Paired
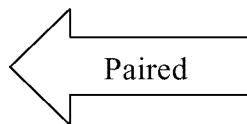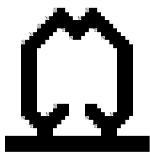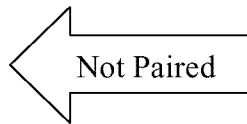
44

SAM

Friendly

Hostile

Not Paired

Paired
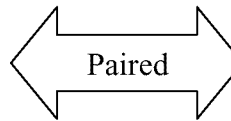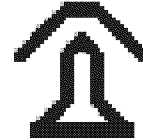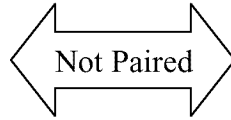
45

Cruise Missile/Other Missiles

Friendly

Hostile
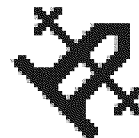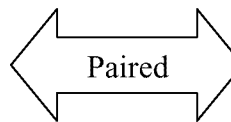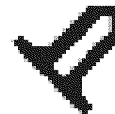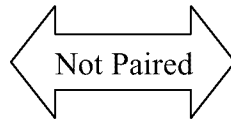
Not Paired

Paired

46

Air Base

Friendly   **Hostile**
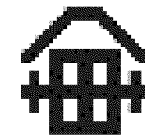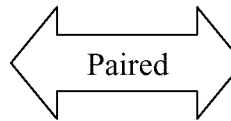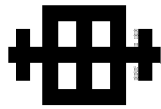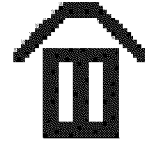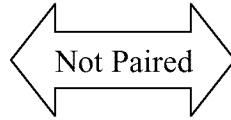
Not Paired

Paired

47

City

Friendly   **Hostile**

Not Paired

Paired

48

93
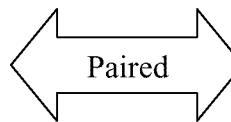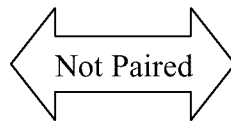
Navy Carrier

Friendly
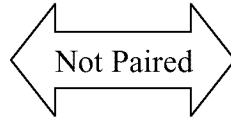
Hostile
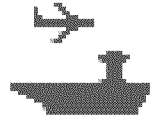
Not Paired

49

Navy Submarine

Friendly
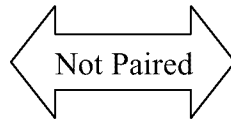
Hostile

Not Paired

50

Navy Surface Combatant

Friendly   Hostile
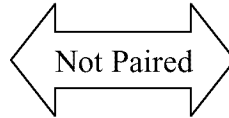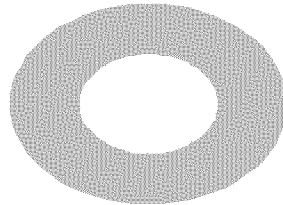
Not Paired

51

Cap Location

Friendly / Not Paired

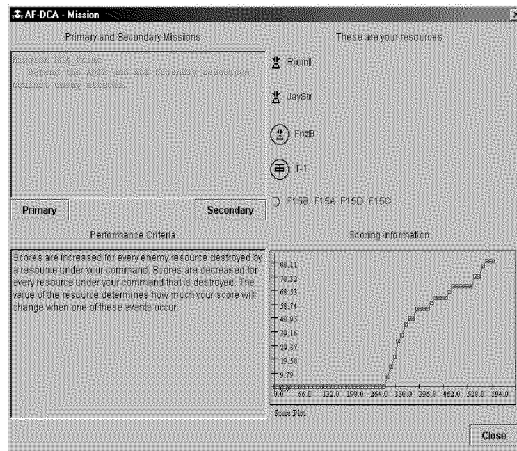52

95

Way Point

Friendly / Not Paired

53

Resource Pairing Rules

- Pairing = engagements between hostile and friendly resources
- Paired are:
  - Friendly resources which have Target, Tank, or RTB order
  - Hostile resources which are being targeted
  - Any targeted city or base
  - Friendly resource with a tanking order
  - Friendly resource with an RTB order

54

96

Mission Window

- Offers information in accordance with one's WD role

- Provides the user with primary and secondary missions

- Informs the user of scoring rules

- Provides a list of resources and scoring graph

55

On to First Practice Session

57

Intelligent Agent Tool

- Provides "best" targeting option based on current resources and threat threat level.

- Allows for faster and more efficient resource allocation

- Studies show, inexperienced WD score as well as experienced WD when using recommendations

- Developed through Subject Matter Experts (SMEs)
  - AWACS Weapons Directors helped design the Decision Support Algorithms

58

Activate the Agent (Pre set for you)

59

58

Manually accept a single recommendation

* Make sure the agent is enabled

* Receive recommendations

* Click on a recommendation

* Recommendation is accepted

60

Make sure the agent is enabled

51
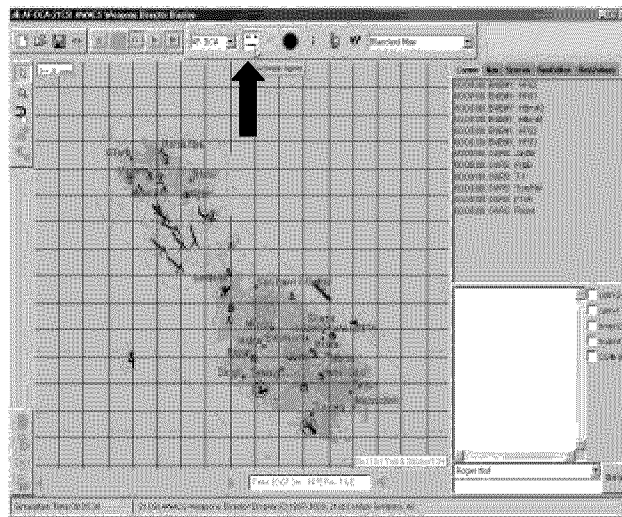
Receive recommendations
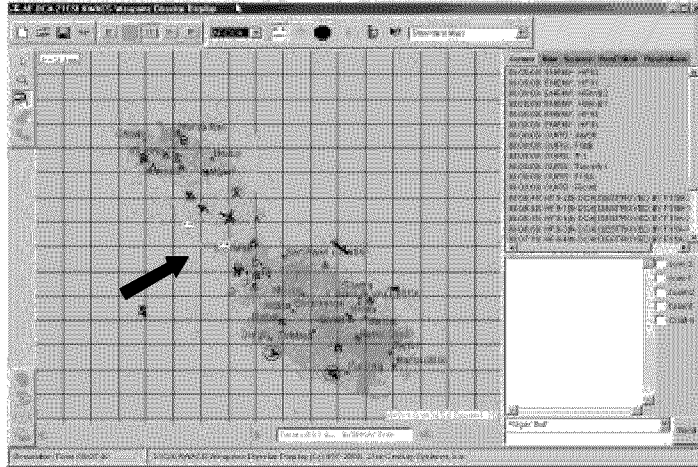
63

Click on a recommendation
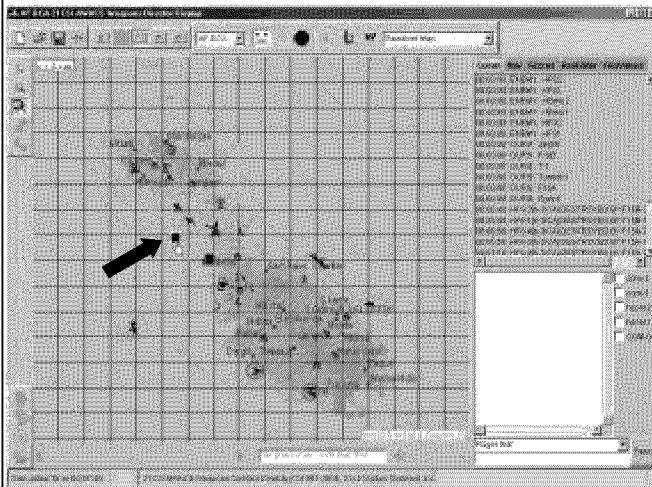
Right click displays recommendation rationale.

Left click accepts recommendation

Recommendations only active for a few seconds

64

Recommendation is accepted

65

Manually accept
all recommendations

• Activate the Agent

• Receive Recommendations

• Accept All Recommendations

66

101

Activate the Agent

67

Receive Recommendations

68

102

Accept all recommendations

Bibliography

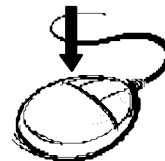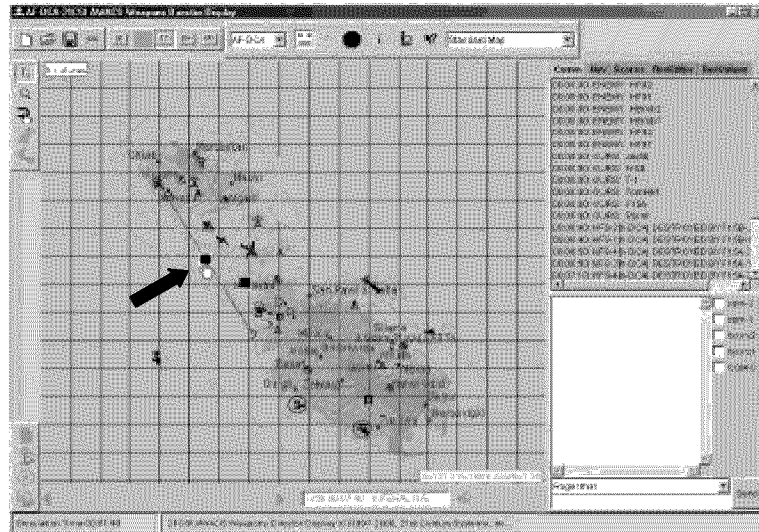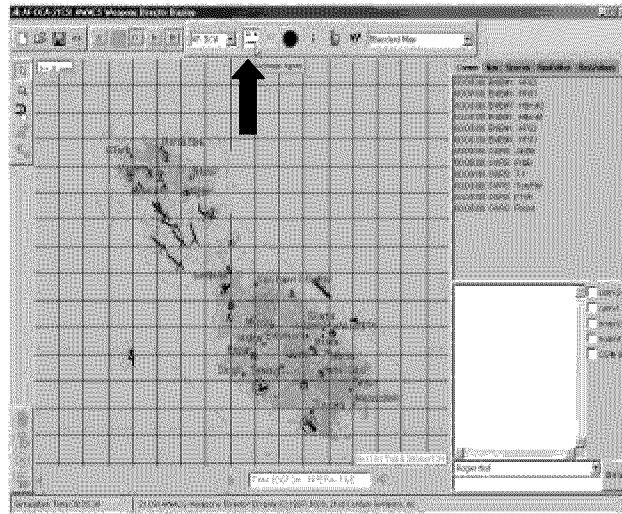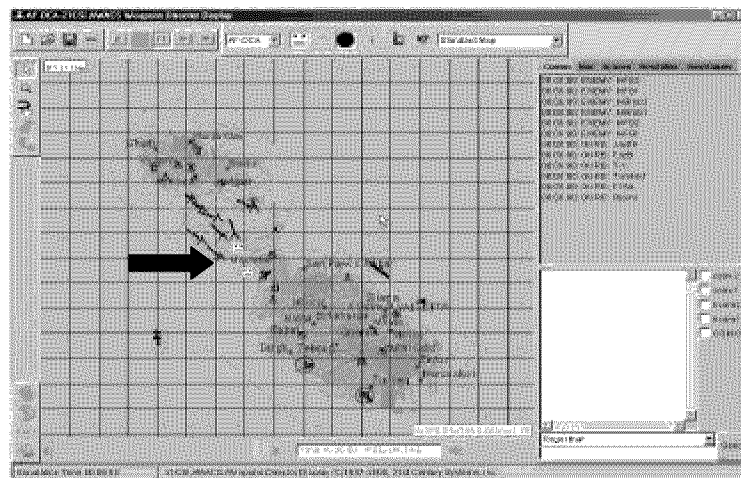Air Command, Control, Intelligence, Surveillance, and Reconnaissance Command
    (AC2ISRC). *Mission Brief.* pag 42. 4 May 1999.

Allison, Grahm T. *Essence of Decision: Explaining the Cuban Missile Crisis.* Boston MA:
    Little, Brown and Company, 1971.

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

Bearden, James. *Command and Control: Enabling The Expeditionary Aerospace Force.* Air
    Command and Staff College, 2000.

Bergstrand, Brad. "Situating the Estimate: Naturalistic Decision-Making as an Alternative to
    Analytical Decision-Making in the Canadian Forces." unpublished article. n. pag.
    http://www.cfcsc.dnd.ca/irc/nh/nh9798/0021.html. 24 June 2001.

Bisantz, Ann M and others. *Empirical Investigations of Trust-Related System Vulnerabilities
    in Aided, Adversarial Decision-making.* Center for Multi-Source Information Fusion,
    Department of Industrial Engineering. State University of New York at Buffalo,
    Amherst NY, 2000.

Bonoma, T. V. "Conflict, Cooperation, and Trust in Three Power System," *Behavioral
    Science*, 21(6): 499-514 (1976).

Boyd, John R. "A Discourse on Winning and Losing," Unpublished set of briefing slides
    available at Air University Library, Maxwell AFB AL, 1987. .

Cannon-Bowers, Janis, A., Eduardo Salas, and John Pruitt, S. "Establishing the Boundaries
    of a Paradigm for Decision-Making Research," *Human Factors*, 38:2 193-205 (1996).

Collyer, Stanley C., and Gerald S. Malecki. "Tactical Decision Making Under Stress:
    History and Overview," In *Making Decisions Under Stress*, edited by Janis A.
    Cannon-Bowers and Eduardo Salas, 3-15. Washington DC: American Psychological
    Association, 1998.

Conjeo, R., and Wickens, C.D. "The effects of highlighting validity and feature type on air-
    to-ground target acquisition performance." University of Illinois Institute of Aviation
    Technical Report ARL-97-11/NAWC-ONR-97-1. 1997.

Denning, Dorthy E. *Information Warfare and Security.* Reading MA: Addison-Wesley, 1999.

Department of Defense. *Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations.* Joint Publication 6-0. Washington, DC. 1995.

Department of Defense. *Joint Doctrine for Command and Control Warfare.* Joint Publication 3-13. 17 February 1996.

Department of Defense. *Joint Doctrine for Information Operations.* Joint Publication 3-13. 9 Oct 1998.

Department of the Air Force. *Compendium of Communications and Information Terminology.* AF Directive 33-303. Washington: HQ USAF, 1 November 1999.

Department of the Air Force. *Air Force Doctrine Document: Information Operations.* AFDD 2-5. Washington: HQ USAF, 5 August 1998.

Devore, Jay L. *Probability and Statistics for Engineering and the Sciences*, Pacific Grove CA: Duxbury, 2000

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

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.

Fadok, David S., John Boyd, and Warden John. *Air Power's Quest for Strategic Paralysis.* Maxwell Air Force Base AL: Air University Press, 1995.

Fields, Gregory S. *The Effect of External Safeguards on Human-Information System Trust in an Information Warfare Environment.* MS thesis, AFIT/GIR/ENV/01M-07. School of Engineering and Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, March 2001.

Fleeger, Daniel. "Threats to Information Systems on The Rise," Air *Force Link.* Air Force Office of Special Investigation. http://www.af.mil/news/Apr2001/n20010430_0582.shtml. 30 April 2001.

Fogg, BJ, and Hsiang Tseng. "The Elements of Computer Credibility." *Conference on Human Factors in Computing Systems.* 80-87. Pittsburgh PA: ACM, 1999.

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).

Hoffman, K A. *Trust and Performance with Intelligent Agent Technology: Implications for Human Interactions.* MS thesis, Department of Psychology, University of South Florida, 2000.

Holsapple, C. W., and Whinston, A. B. *Decision Support Systems: A Knowledge-based Approach,* Minneapolis MN: West Publishing Co., 1996.

Howard, Micheal, and Peter Paret. *Carl von Clausewitz: On War, Ed. and Trans.* Princeton, N.J.: Princeton University Press, 1984.

James, F. Roberts. "C4ISR for Dummies," Surface *Warfare.* (November/December 1999).

Jina, Jiun-Yin. and others. *Foundations for an Empirically Determined Scale of Trust in Automated Systems.* Center for Multisource Information Fusion no. CMIF-1-98, State University of New York at Buffalo, 1998.

Klein, G A. "Naturalistic Models of C3 Decision-making." In *Science of Command and Control,* edited by Stuart E. Johnson and Alexander H. Levis, 86-92. Washington, DC.: AFCEA International Press, 1988.

Klein, G. A. and others. *Decision-making in Action: Models and Methods.* Norwood NJ: Albex Publishing Corp., 1993.

Klein, Gary, and David Klinger. "Naturalistic Decision-Making," *Crew System Ergonomics Information Analysis Center Gateway* 2:1 (Winter 1991).

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.

Lee, J., & Moray, N. "Trust, self-confidence, and operators adaptation to automation," *International Journal of Human-Computer Studies, 40*(1) 153-184 (1994).

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

Libicki, Martin. *What is Information Warfare?* National Defense University. Institute for National Strategic Studies, 1995.

Llinas, James and others. *Studies and Analyses of Vulnerabilities in Aided Adversarial Decision Making: Final Report, 1 April 1996- 1 February 1997.* Contract AFRL/HE-WP-TR-1998-0099. Buffalo NY: State University of New York at Buffalo, February 1998.

Lyles, M.A., and H. Thomas. "Strategic Problem Formulation; Biases and Assumptions Embedded in Alternative Decision-Making Models," *Journal of Management Studies*, 25:2 131-45 (1988).

Lyons, Michael, D. "A Test Paradigm for War game 2000." Unpublished paper. n. pag. http://www.dodccrp.org/Proceedings/DOCS/wcd00000/wcd000e2.htm August 2000.

March, James, G and H. Simon, *Organizations,* New York: Wiley, 1958.

Marsden, Chris. "Chinese Embassy Bombing." Online article. http://members.tripod.com/kosov099/chinese.htm. 31 May 2001.

Mayer, Daryl. "Keeping Air Force Secrets Secret." Air Force news article. http://www.af.mil/news/jun2000/n20000621_000943.htm. June 21 2000.

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.

Mengxiong, Chang. "Weapons of the 21st Century." In *The Revolution in Military Affairs. Chinese Views of Future Warfare*, no date.

Metz, Steven. *Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare.* Strategic Studies Institute, U.S. Army War College. Carlisle PA, 2000.

Mosier, K. L., Skitka, L. J., Heers, S. & Burdick, M. D. "Patterns in the use of cockpit automation," in M. Mouloua & J. Koonce (Eds.), *Human-automation interaction: Research and Practice.* Hilsdale NJ: Lawarence Erlbaum Assoc., Inc 167-173 (1997).

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

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

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.

Myers, Laura. "Pentagon Computers Vulnerable." The Associated Press article from march 1999 http://abcnews.go.com/sections/tech/dailyNews/hackerspentagon990322.html 3 June 2001.

Nass, C., Fogg, B. J., & Moon, Y. "Can Computers Be Teammates?" *International Journal of Human-Computer Studies,* 45(6), 669-678 (1996).

Orasanu, J, and Connolly T. "The Reinvention of Decision-making." In *Decision Making in Action*, edited by G. A. Klein, J. Orasanu, and R. & Zsambok Calderwood, C.E, 3-20. Norwood NJ: Albex Publishing Corp., 1993.

O'Hare, D. "The "Artful" Decision-maker: A Framework Model for Aeronautical Decision-Making," *The International Journal of Aviation Psychology*, 2: 75-91 (1992).

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

Randel, J M, and Pugh H.L. "Differences in Expert and Novice Situation Awareness in Naturalistic Decision-making," *International Journal of Human-Computer Studies,* 45:5: 579-97 (1996).

Rempel, J.K., Holmes, J.G., & Zanna, M.P. "Trust in close relationships," *Journal of Personality and Social Psychology,* 49: 95-112 (1985).

Riley, V. "Operator reliance on automation: Theory and data." In Parasuraman, R. & Mouloua, M. (Eds.), *Automation and Human Performance,* 19-35. Mahwah NJ: Lawrence Erlbaum Associates (1996).

Roman, Gregory A. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide." In *Essays on Strategy*, edited by Institute for National Strategic Studies, 1996.

Sall, John., Lehman, Ann and Creighton, Lee. *JMP Start Statistics: A Guide to Statistics and Data Analysis*, Pacific Grove CA: Duxbury, 2001.

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

Seong, Younho, and Ann M. Bisantz. "Modeling Human Trust in Complex, Automated Systems Using a Lens Model Approach." Abstract in, Studies *and Analyses of Aided Adversarial Decision Making,* 95-100 (1998).

Sheridan, T. B. "Computer Control and Human Alienation," Technology *Review,* 61-73 (October 1980).

Sheridan, T. B. "Trustworthiness of Command and Control Systems," *IFAC Man Machine Systems,* 427-431 (1988).

Sheridan, William. "The Paradigm Shift of the Information Age," An online article. http://www3.sympactico.ca/cypher/effects.htm. 21 August 2000.

Skitka, Linda J., Kathleen L. Mosier. "Does automation bias decision making?" *International Journal of Human-Computer Studies,* 51, 991-1006 (1999).

Skitka, Linda J., Kathleen L. Mosier. "Automation Use and Automation Bias," In *Proceedings of the Human Factors and Ergonomics Society 43rd Annual Meeting.* (1999).

Skitka, Linda J., Kathleen L. Mosier, and Mark Burdick. "Accountability and Automation Bias," International *Journal Human-Computer Studies,* 52: 701-17 (2000).

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

Sprague, R.H, and Carlson E.D. *Building Effective Decision Support Systems.* Englewood Cliffs NJ: Prentice-Hall, 1982.

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

Tseng, Shawn, and Fogg B. J. "Credibility and Computing Technology," Communications *of The ACM,* 42:5: 39-45 (May 1999).

Tyler, Robert R. "Human Automation Interaction - A Military User's Perspective," 1997.

Weick, Karl E. *Sensemaking in Organizations.* Thousand Oaks: SAGE Publications Inc, 1995.

Weick E., Karl, and Karlene Roberts H. "Collective Mind in Organizations: Heedful Interrelating on Flight Decks," Administrative *Science Quarterly,* 38: 357-81 (1993).

Whitehead, YuLin. "Information as a Weapon: Reality versus Promises." Essay. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj97/fal97/whitehead.html. 12 June 2001.

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.

Wickens, C.D., Mavor, A., Parasuraman, R., and McGee, J.M. *The future of air traffic control: Human Operators and Automation.* Washington, DC: National Academy Press. 1998.

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

REPORT DOCUMENTATION PAGE

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 the collection of information, including suggestions for reducing this 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 an 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) 26-03-2002	2. REPORT TYPE Master's Thesis	3. DATES COVERED (From – To) Aug 2000 – Mar 2002

4. TITLE AND SUBTITLE TASK LOAD AND AUTOMATION USE IN AN UNCERTAIN ENVIRONMENT	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) Daly, Mark, A., Captain, USAF	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S) Air Force 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/GAQ/ENV/02M-05

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) AFOSR Dr. Robert L. Herklotz 801 N. Randolph St. Room 732 Arlington, VA 22203-1977 703-696-6565	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
The purpose of this research was to investigate the effects that user task load level has on the relationship between an individual's trust in and subsequent use of a system's automation. Automation research has demonstrated a positive correlation between an individual's trust in and subsequent use of the automation. Military decision-makers trust and use information system automation to make many tactical judgments and decisions. In situations of information uncertainty (information warfare environments), decision-makers must remain aware of information reliability issues and temperate use of automation if necessary. An individual's task load may have an effect on his use of a system's automation in environments of information uncertainty.

It was hypothesized that user task load will have a moderating effect on the relationship between system automation trust and use. Specifically, in situations of information uncertainty (low trust), high task load will have a negative effect on the relationship. To test this hypothesis, an experiment was conducted in which system automation trust and individual task load were manipulated. The findings from the experiment support the positive relationship between automation trust and automation use found in previous research and suggest that task load does have a negative effect on the positive relationship between automation trust and automation use.

15. SUBJECT TERMS
Task Load, Human-Automation Trust, Information Warfare, Automation Use, Decision Making

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Lt Col David Biros, ENV
a. REPORT U	b. ABSTRACT U	c. THIS PAGE U	UU	120	19b. TELEPHONE NUMBER (Include area code) (937) 255-3636, ext 4826; e-mail: Daivid.Biros@afit.edu