TRAINING EFFECTS ON JUDGMENT ACCURACY IN A COMPUTER-MEDIATED ENVIRONMENT

THESIS

Mark M. Lankowski, First Lieutenant, USAF

AFIT/GIR/ENV/03-10

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright Patterson Air Force Base, Ohio

AFIT/GIR/ENV/03-10

TRAINING EFFECTS ON JUDGMENT ACCURACY IN A COMPUTER-MEDIATED 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 Information Resource Management

Mark M. Lankowski, B.S.

First Lieutenant, USAF

March 2003

AFIT/GIR/ENV/03-10

TRAINING EFFECTS ON JUDGMENT ACCURACY IN A COMPUTER-MEDIATED ENVIRONMENT

Mark M. Lankowski, B.S.
First Lieutenant, USAF

Approved:

//SIGNED//	3 March 2003
David P. Biros (Chairman)	date
//SIGNED//	3 March 2003
Joey F. George (Member)	date
//SIGNED//	3 March 2003
Kent Marett (Member)	date

Acknowledgements

I would like to thank my family and friends for constantly providing the encouragement, motivation, and patience that I needed to complete this effort. Lieutenant Colonel David Biros, Dr. Joey George, and Kent Marett were the finest thesis committee a graduate student could ask for. Thank you for the detailed feedback and guidance throughout the entire process: from FSU to AFIT to Keesler and back to AFIT again. I would also like to thank the faculty and students at AFCOT, Tony Maddin and AFIT SC, and my classmates at AFIT for all their support.

Without a doubt, the deception detection research group was essential to completion of the Keesler experiment and this effort. Thank you for all the fun, teamwork, and help. Only they can truly understand when I quote, "Going once…, going twice…, SEE-YA!"

Mark M. Lankowski

Table of Contents

Page

List of Figures

List of Tables

Abstract

The United States Air Force (AF) has named Information Superiority the core competency "upon which all the other core competencies rely". In order to achieve Information Superiority, deceptive communication must be minimized. According to researchers, deception occurs when communicators control the information contained in their messages to convey a meaning that departs from the truth. This research draws on Biros, George, and Zmuds' (2002) deception research model to determine if training to detect deception will improve a person's deception detection performance in a computer-mediated environment. A longitudinal experiment was conducted with AF participants (N=119) where three separate training plans were provided as the treatments, and measurements of the participants' deception detection performance were taken before and after each of the three treatments. Each measurement was taken in the form of six judgment scenarios provided through three forms of computer-mediated communication. Partial support was found for training improving deception detection performance and reducing the number of false alarms in a computer-mediated environment, based upon the first training treatment and a combination of the first and second training treatments. However, contradictory results came from the second and third training treatments. The most significant finding was that the performance of AF participants attempting to detect deception in a computer-mediated environment could be improved by a training session. Further research should explore the best training methods to improve the deception detection performance of all AF members in order to achieve the goal of Information Superiority.

TRAINING EFFECTS ON JUDGMENT ACCURACY IN A COMPUTER-MEDIATED ENVIRONMENT

I. Introduction

Background

According to Joint Vision 2020, information, information processing, and communications networks are at the core of every military activity (Joint Vision 2020, 2000). Information is critical to success for the Department of Defense (DoD). Every member of the DoD makes decisions based on information. However, commanders of military units within the DoD make decisions that directly affect the defense of our nation. "The commander with better information holds a powerful advantage over his enemy" (Fogelman, 1995:7). Since information is so valuable, the Air Force has named Information Superiority the core competency "upon which all the other core competencies rely" (AFDD 2-5, 1998:2). Information Superiority is defined as, "The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same" (Joint Vision 2020, 2000:8).

Information flows through different media. Media defined by Webster's Dictionary is "an intervening substance through which something else is transmitted or carried on." Examples of the different forms of media that information flows through include: face-to-face communication, voice communication over distances (telephones), text communication (letters, e-mail, etc.), video, and images (Baltes, Dickson, Sherman, Bauer, and LaGanke, 2002). Nearly every form of media can be processed using a computer, i.e. computer-mediated communication (CMC). CMC has become a key

enabler for communications within the private sector, allowing for new ways to accomplish work for groups separated by time and space (Baltes et al., 2002). Furthermore, the military realizes the benefits of CMC. For example, a commander may not be able to have face-to-face communication with a fellow commander on the other side of the world, but through the use of technology, a video-teleconference could be established to simulate a face-to-face communication. As this example shows, CMC provides a powerful tool for commanders, and thus for the DoD in defending our nation. A commander can collect and process all the information he/she needs to make a decision through a computer mediated environment.

Information and the computer mediated environment that allow commanders to collect, process and disseminate information are key enablers to achieving the goal of "decision superiority." However, while "decision superiority" offers many advantages, it also creates vulnerabilities that our adversaries can exploit (Joint Vision 2020, 2000). Information, and the media used to deliver it, need to be protected to maintain "decision superiority." This phenomenon renders Information Assurance a necessity (AFDD 2-5, 1998).

Information Assurance is defined as "…those measures to protect and defend information and information systems by ensuring their availability, integrity, authenticity, and nonrepudiation (ability to confirm source of transmission and data)" (AFDD 2-5, 1998). Information Assurance covers a broad spectrum of information and information technology defense. The spectrum ranges from physical security of the information technology (e.g., guarding against unauthorized access), all the way to information manipulation by "trusted" users of the information. AFDD 2-5 states that manipulation

of information systems can cause incorrect information to influence a commander's decision making or even destroy a commander's confidence in his/her information systems. Strategic information manipulation has also been seen as an important area for study within organizations in the private sector (Zmud, 1990).

Deception is one type of information manipulation which is particularly devastating to decision superiority. According to researchers, deception occurs when communicators control the information contained in their messages to convey a meaning that departs from the truth (Burgoon and Buller, 1996). However, it has been estimated that the receiver of a deceptive communication has only a 50 percent chance to successfully determine whether or not that communication was deceptive (DePaulo and DePaulo, 1989; Ekman and O'Sullivan, 1991; Feeley and deTurck, 1995).

Researchers have shown that individuals trained on reliable cues of deception (e.g., adaptors, pauses, speech errors) are capable of improved deception detection performance (deTurck, Harszlak, Bodhorn, and Texter, 1990; deTurck, 1991; Porter, Woodworth, and Birt, 2000; Zuckerman, Koestner, and Alton, 1984). Furthermore, error detection from stored data may be improved (Klein and Goodhue, 1997). Researchers have recently begun to study training to improve deception detection in a computer-mediated environment because training has been able to improve deception detection in face-to-face situations.

Problem Statement

Since successful deception detection is so difficult to achieve in any environment, it presents an excellent opportunity for academic study. The research proposed here will develop an answer to the question, "Does training improve deception detection

performance in a computer-mediated environment?" In order to improve the odds of detecting deception and achieve "decision superiority," training users to detect deception will be accomplished. Specifically, the training will focus on teaching individuals how to detect deception in a computer-mediated environment. CMC offers many new opportunities for information to be disseminated and collected, but deception will continue to be a problem when attempting to achieve "decision superiority."

Scope

Deception and the study of its detection are broad areas of study. This thesis effort will utilize a set of three training plans developed by experts (George, Biros, and Burgoon, 2002) in the Communications research discipline to test the effects of training on deception detection performance. The first training plan focuses on deception detection in general, the background of research accomplished on deception detection specifically, as well as an overview of what researchers show to be the best methods for detecting deception. The second training plan focuses on the indicators that are evident during a deceptive communication (deTurck et al., 1990; Kalbfleisch, 1985; Zuckerman and Driver, 1985). The final training plan describes the cognitive heuristics, or mental short cuts, that accompany deceptive communications, and how to utilize them to detect deception (McCornack and Parks, 1986; Stiff, Kim, and Ramesh, 1992). These three training plans will be measured on the level of deception detection performance the participants' exhibit upon completion of each training session.

Tests including deceptive and non-deceptive examples of communication will measure the effects of the training plans. The examples of communication will be provided in a computer-mediated environment. By this, I mean that each participant will

take the test before and after each training plan on a computer. The examples of communication will include video, audio and text scenarios, on which the participants will make veracity judgments. Using these forms of CMC will facilitate a further understanding of deception and deception detection, and the CMC constructs will be defined in Chapter Two. Biros, George, and Zmuds' (2002) research model was used to guide the development of this thesis effort (see Figure 1) because it implies causal relationships between training and deception detection accuracy.

Once the experiment has been completed, the results will be analyzed and the effects that each training plan had upon deception detection performance will be shown.

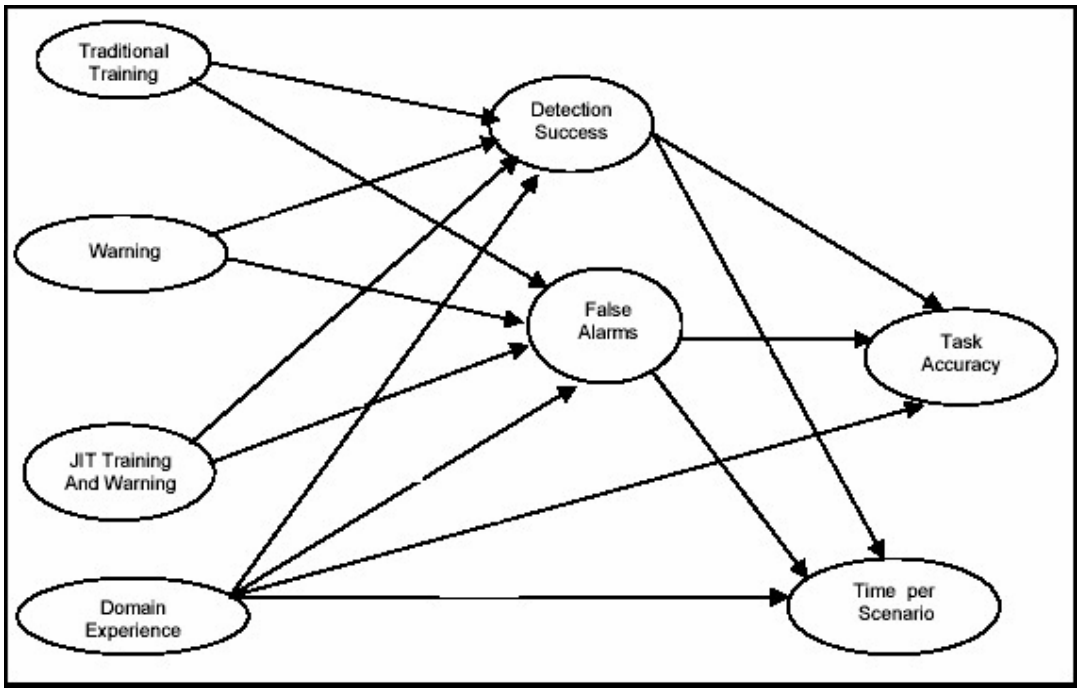

Figure 1. Theoretical Research Model

Research Contribution

If the training plans improve deception detection performance, then the Air Force Office of Scientific Research (AFOSR) will have another tool to improve Information Assurance within the Air Force and eventually the DoD. With improved Information Assurance, the Air Force will be more prepared to successfully execute its mission objectives to fly, fight and win. The research contribution for academics will include the deception detection body of knowledge being expanded, as well as the provision of empirical support to those researchers studying training effects on deception detection performance in a computer-mediated environment. Academics and practitioners alike will reap benefits within the Air Force community because the study will be conducted on active duty Air Force officers.

Summary

This chapter discussed the importance of information, the role that CMC plays in disseminating information to decision-makers, and the catastrophic implications of deception altering decision-makers' information. Furthermore, because of these factors deception detection is critical to Information Assurance (AFDD 2-5, 1998). The scope of this research was briefly outlined with respect to the model that Biros et al. (2002) proposed.

The following chapter will review the literature on deception, deception detection, computer-mediated communication, training, and specific training to improve deception detection performance. Specific hypotheses will be proposed concerning the training effects on deception detection performance in a computer-mediated environment. Chapter Three will discuss the methodology used to conduct the testing of the hypotheses

formulated at the end of the following chapter. Chapter Four will provide the results and analysis of the experiment proposed in Chapter Three. Chapter Five will present a summary of the findings, limitations of the study, implications for the Air Force, and suggestions for further research.

II. Literature Review

Overview

It has been estimated the receiver of a message has only slightly better than chance (DePaulo and DePaulo, 1989; Ekman and O'Sullivan, 1991; Feeley and deTurck, 1995) to successfully conclude whether the communicator is being deceitful or telling the truth. According to researchers, "deception" occurs when communicators control the information contained in their messages to convey a meaning that departs from the truth (Burgoon and Buller, 1996). A "lie" on the other hand is to say something that is not true or to imply a false idea. Deception and lies constitute the realm of information falsifications: "misdirection, concealment, omissions and exaggerations," (Ebesu and Miller, 1984:418) of the truth. Within the Air Force, and to a larger extent the entire Department of Defense, commanders rely upon information to make decisions (Joint Vision 2020, 2000). Information falsifications provided to a commander may reduce the quality of a decision. Therefore, it is pertinent that information falsifications within a message are detected before a commander uses deceptive information to make a decision. A human's ability to evaluate a message for information falsifications is the basis for deception detection.

The ability to detect deception has been studied for years (Biros et al., 2002; Buller and Burgoon, 1996; deTurck and Miller, 1990; McCornack and Parks, 1986; Zuckerman and Driver, 1985; Porter et al., 2000; Zuckerman et al., 1984). This chapter discusses past research in this area and explores deception detection for the purpose of decision-making superiority. Next, the research on computer-mediated communication (CMC) will be reviewed. In addition, this chapter describes some of the types of human

deception detectors that are in use today, discusses where the field is headed and how deception detection is an integral part of information warfare. Finally, training will be discussed in terms of how it may be used to improve deception detection performance. Based on the literature reviewed, the definitions provided, and past theoretical models an adapted model for the study of training to improve deception detection performance in a computer-mediated environment will be presented along with hypotheses based on the adapted model.

Deception Detection

While there are currently no theories posited to aid deception detection in a computer-mediated environment, future research might build on the well-known human-to-human deception detection theories of information manipulation theory (McCornack, 1992) and interpersonal deception theory (Burgoon and Buller, 1996). Interpersonal deception theory (IDT) is a framework for predicting and explaining the dynamics of deception during human-to-human interaction where a major factor in deception or deception detection success is a person's communication skills (Burgoon and Buller, 1996). Information manipulation theory (IMT) takes a different approach, where deceptive messages derive from concealed violations of "conversational maxims" (McCornack, 1992:4). Both of these theories will be examined and related within the framework of deception detection in a computer-mediated environment.

Interpersonal Deception Theory (IDT)

> "Deceivers must accomplish numerous communication tasks simultaneously. They must plan and encode credible verbal messages while projecting a believable nonverbal image; they must manage their emotions; they must attend to their partner and keep the conversation running smoothly; they must send desired relational messages to their partner and respond appropriately to partner

> messages; and they must be discreet about any intentions to influence or deceive the partner (Burgoon and Buller, 1994:155)."

The communication tasks described within the definition of IDT can all be synthesized into a communicator's social skills. According to IDT, the more socially skilled one is as a communicator, the better he/she will be at deceiving or detecting deception within a communication. That is, if a sender is trying to deceive a receiver, there is a positive relationship between deception success and a sender's social skills. Furthermore, if a receiver is trying to detect deception of a sender, there is a positive correlation between deception detection success and a receiver's social skills. Empirical studies exist supporting IDT in human-to-human deception detection capability (Burgoon and Buller, 1996; Burgoon and Buller, 1994), but taking the next step to deception detection in a computer-mediated environment is a difficult undertaking. Social skills can be easily observed in a face-to-face interaction, but not so readily in a computer-mediated interaction. Information manipulation theory (IMT) provides the next logical step to deception detection in a contextual format, in which a human is interacting with a form of media as opposed to another human.

Information Manipulation Theory (IMT)

IMT provides four maxims of communication that when violated can be considered attempts at deception in communication. These maxims can be applied to any media, so IMT is a more general theory than IDT, where face-to-face deception detection is the main focus. The four maxims are (McCornack, 1992:9-13):

> **Quantity.** The maxim of Quantity refers to a person's expectations that a conversation will be as informative as possible. Information omission is not expected. If information is omitted, then there is an expectation of deception in the communication.

Quality. The maxim of Quality refers to a person's expectation of being presented with information that is truthful and complete. Obviously, if information is not truthful or the information is purposefully ambiguous, then there is deception in the communication.
Relation. The maxim of Relation illustrates the expectation of contributing relevant information to a conversation. That is, a communication is expected to "get to the point." If the communication avoids relevant information, then there is deception in the communication.
Manner. The maxim of Manner relates to how things are said rather than what is said. For example, if a user of a system expects a communication in a certain format, and that communication is not in the expected format, then there is deception in the communication.

IMT relies upon maxims of communication, where IDT relies more on the social skills of both the sender and receiver (Burgoon et al., 1995). Because IMT relies upon maxims of communication, this theory can be more aptly applied to detect deception in a computer-mediated environment. For example, a military contracting officer attempting to detect deception in an e-mail message from an unscrupulous civilian contractor could use IMT to study the message. The military officer would check for omitted data from the contractor's message through the Quantity maxim, or whether or not the message included relevant information through the Relation maxim. However, the use of IDT would not provide a reliable way for determining deception because of the medium that the message was sent, in this case e-mail. That is not to say that the two theories are completely unrelated, but that they are targeted for different media. Both theories emphasize the relationship between sender and receiver, but they are applied differently through the medium used for communication.

Deception Detection Cues

A study of deception detection would not be complete without evaluating all of the cues being provided by the potential deceiver, or sender, via analysis of their

nonverbal, verbal, physiological and psycho-physiological indicators. Conscious and unconscious signals indicate probing points where further investigation is required to ascertain whether or not the sender is attempting to deceive or lie to the receiver of a message (Buller and Burgoon, 1994; Burgoon et al., 1995; DePaulo, 1992; Zuckerman and Driver, 1985).

According to Zuckerman and Driver (1985), nonverbal cues that are significantly associated with deception include the following: increased pupil dilation and blinking rates, less facial segmentation (feigned versus genuine smiles), more bodily segmentation (restless trunk and limb movement) and adaptors. Adaptors are activities in which the sender is moving his/her hand while touching their body, such as scratching (deTurck and Miller, 1985). Zuckerman and Driver (1985) also identified that deceptive messages contain the following paralinguistic (i.e., the set of nonphonemic properties of speech, such as speaking tempo, vocal pitch, and intonational contours, that can be used to communicate attitudes or other shades of meaning – Webster's Dictionary) cues: shorter response length, higher speech pitch, and increased speech errors, and hesitations. Nonverbal cues must be studied along with verbal cues to detect deception.

Verbal cues are obtained from the actual speech or written language. According to Zuckerman and Driver (1985), verbal behaviors associated with deception include: more negative statements, increased speech errors, more speech hesitations, and increased leveling (overgeneralizations). Conveying the truth up to a certain point and the use of stalling tactics, as well as the exclusion of negative aspects of the story and an unwavering desire to fill the silence of a room (Navarro and Schafer, 2001) are further examples of verbal indicators of deception.

Deception occurs in prominent locations where the verbal and nonverbal cues may be evident. According to Henahan, investigators analyzed President Clinton's testimony in which he denied any sexual relationships with his intern, Monica Lewinsky. The analysis measured 20 verbal and nonverbal indicators that were observed. The analysis reported large increases in President Clinton's verbal and nonverbal behavior including: leaning, drinking and swallowing, hand-to-face touching, averting the gaze, reduction in blinking, qualifiers and modifiers, expanded contractions, denials, speech errors and stuttering (Henahan, 1999). The percentages of increased indicators ranged from 63% to 1733%, with the majority of percentages over 100%.

Examples of written deception are continuously being presented in reference to the alcohol and tobacco industries (Hacker and Steinhardt, 1997). Currently, the wine industry is reporting coronary health benefits of drinking moderate amounts of wine. The Center for Science in the Public Interest is publicly opposing this statement saying that the Wine Industry failed to report significant results of the study. Some of the omitted statements include the researcher inferring a potential link between breast cancers and drinking (even at moderate doses) and that several people react poorly overall to alcohol and can easily become addicted.

Similarly, the Non-Smokers Rights Association (NSRA) has pointed out the tobacco industry's deceitfulness in labeling cigarettes as "light" (low in tar content) when in fact the contents of light cigarettes are almost identical to regular cigarettes. The NSRA believes that smokers concerned about their health turned to this "light" product when they may have quit had they realized there really was not a significant difference in

tar content. Deception occurs in many industries and to many audiences, but detecting the deception is extremely difficult.

The final indicators to deception are physiological and psycho-physiological. Physiological indicators include galvanic skin resistance (e.g., sweaty palms) as well as breathing and heart rates. The psycho-physiological indicator is brainwave activity, or cognitive processing (Farwell and Richardson, 1993). However, unless there is a way to measure these psycho-physiological and physiological indicators from a human message sender during a CMC, they are useless in detecting deception in a computer-mediated environment.

Decision-Making in a Computer-Mediated Environment

Choosing the appropriate medium for communication is an important undertaking. This is especially true as the military relies more and more on information systems to accomplish daily tasks. The following quotation from Air Force Doctrine Document 2-5 illustrates this concept,

> "The Air Force's increased ability to access, process and store information, coupled with its ever-increasing dependence on information systems and information infrastructures have driven the Air Force to reexamine and redefine how it integrates information-related activities into its functions (AFDD 2-5, 1998:5)."

Communication media differ in their ability to facilitate understanding. Media can be identified as low or high in "richness" based on their capacity to impart meaning. Daft, Lengel, and Trevino (1987) ranked media channels from high to low in their capacity to impart meaning: (1) face-to-face, (2) telephone, (3) addressed documents, and (4) unaddressed documents. The notion of media "richness" led researchers to propose a Media Richness Theory (Daft and Lengel, 1986 and Daft et al., 1987). They defined

media richness as the ability of information communicated on the medium to reduce equivocality, and based it on four criteria: speed of feedback, cue multiplicity, language variety, and personal focus. Media having higher degrees of each of these criteria are considered "richer." Studies have shown that for decision-making, the media chosen for communication made a difference in the outcome of the task performed (Hedlund et al., 1998; Daft et al., 1987; Olaniran, 1995). For the purposes of this thesis effort, computer-mediated communication will entail video, voice and data excerpts from communications that took place in an interview setting. While none of these CMC's is face-to-face, they do range from "rich" media (video) to "lean" media (data) on the continuum of media richness. The choice was made to study CMC because of the increased reliance placed on information technology as a means of communication.

Within the Air Force, "dominating the information spectrum is as critical to conflict now as controlling air and space, or occupying land was in the past, and is viewed as an indispensable and synergistic component of aerospace power" (AFDD 2-5, 1998:5). The United States military's reliance upon information systems exacerbates our vulnerability to deception. Joint Vision 2020 clearly states the importance of information technology to the war-fighter in coming years, and to accomplish this information superiority must be achieved. To ensure that information superiority is attained and sustained, military researchers are expanding the deception detection body of knowledge from IDT and IMT to theories that enhance deception detection within computer-mediated environments. Evolving the current research that explores human-to-human deception detection to increase our military personnel's ability to detect deception when working within a computer-mediated environment to accomplish a mission is critical.

The following examples illustrate how deception could be used to affect our military operations: field informants may omit critical details about suspicious activities, disinformation campaigns (such as before the D-Day invasion in WWII) may direct attention to bogus operations away from real ones, opponents may leak information that exaggerates or downplays the state of their weapons arsenals and make public speeches that conceal their true intentions, intelligence analysts may be equivocal about their confidence in their data or the thoroughness of their analysis. Thus, deception detection research is important in continued development of new ways for our military to ensure information and decision-making superiority. The high priority Joint Vision 2020 is placing on information and decision superiority will continue to push deception detection research forward. Deception detection and deception are also key parts to the information warfare puzzle.

> "Information Warfare is information operations conducted to defend the Air Force's own information and information systems or conducted to attack and affect an adversary's information and information systems. This warfare is primarily conducted during times of crisis or conflict. However, the defensive component, much like air defense, is conducted across the spectrum from peace to war," (AFDD 2-5, 1998:1).

This statement asserts that deception detection is an integral part of assuring our information systems are providing accurate, secure information to the war-fighter both in time of peace and war operations. According to Libicki, there are seven forms of information warfare:

> (*i*) command-and-control warfare, (*ii*) intelligence-based warfare (which consists of the design, protection, and denial of systems that seek sufficient knowledge to dominate the battle space), (*iii*) electronic warfare, (*iv*) psychological warfare (in which information is used to change the minds of friends, neutrals, and foes), (*v*) "hacker" warfare (in which computer systems are attacked), (*vi*) economic information warfare (blocking information or channeling it to pursue economic dominance), and (*vii*) cyber warfare (Libicki, 1995:1).

Deception and deception detection are a part of each and every one of Libicki's seven forms of information warfare, because they both are ways information can be manipulated. Earlier examples provide a framework for scenarios where deception and deception detection could be viewed as one of the seven forms of information warfare.

Deception Detection in a Computer-Mediated Environment

Deception detection research has primarily been focused on human-to-human interactions. This research will continue because there is still much to be learned about detecting deception in human-to-human interactions. However, with the recent explosion of information system (IS) use and human reliance on information systems to accomplish their work, computer-mediated deception detection is becoming the next frontier for deception detection researchers (Klein and Goodhue, 1997; Muir, 1987, Parasuraman, 1987).

Computer-mediated deception detection involves a human interacting with an information system and determining whether the information garnered from the IS was correct or had been tampered with. For example, imagine an air traffic controller, Joe Smith, using an IS to keep track of airspace around a busy airport. Hundreds of planes were taking off and landing, while Joe Smith relied upon an IS to update him if there were any problems with the flight paths (Muir, 1987; Parasuraman 1987). Suppose data in the air traffic control IS was altered to change the elevation of the runway by a malicious deceiver. Would Joe Smith be able to detect the deceptive data, or would he rely on the "trusted" IS to guide the airplanes to land at the airport?

This is an extreme, yet important example. There are a number of problems that can be identified in connection with reliance upon information systems. IS users, like Joe Smith in the example, learn to become dependent upon information systems to do their job. Automation of the air traffic control may lead to user complacency or boredom which would cause the user to accept whatever information the IS was producing as factual, correct data (Millar and Millar, 1997). If Joe Smith was unable to understand that the data had been manipulated in the IS, airplanes may have crashed. User dependence on information systems to meet their occupational needs would make them even more susceptible to information manipulation by a deceiver (Klein and Goodhue, 1997; Muir, 1987, Parasuraman, 1987).

To help improve detection of deception, automated tools have been and still are being investigated to assist the interviewer with the decision process along with more training. The most well known tool currently being used today is the polygraph or lie detector test, which has been tested and used in the United States since 1897. The polygraph has been used to assist with numerous areas of criminal investigations and job interviews carried out by both the private sector and the Department of Defense. The polygraph is a physiological tool that measures respiratory response through collectors placed on the chest and abdominal areas, sweat gland activity through nodes attached to the ring and index fingers, and cardiovascular activity by calculating blood pressure. The principle idea behind this test is that the fear of being caught in the lie creates anxieties and arousals within the body and thus multiple physiological changes. The investigator has the responsibility of collecting and analyzing the nonverbal and verbal communication to perform the overall analysis (Polygraph Clarification Services, 2002).

Training to Improve Deception Detection Performance

As stated in the previous section, there are many tools to aid in deception detection. However, they all measure physiological or psycho-physiological indicators that require the sender of the CMC to be physically analyzed by a machine. It is generally not feasible to analyze the sender of a CMC for physiological or psycho-physiological indicators; therefore another means of deception detection must be sought. Research has shown that training on the reliable verbal and nonverbal indicators of deception may improve a receiver's detection performance (deTurck et al., 1990; deTurck, 1991; Porter et al., 2000; Zuckerman et al., 1984). Therefore, the lack of physiological or psycho-physiological indicators in a CMC may be overcome. However, CMC removes a receiver's ability to examine all of a sender's behaviors (Buller and Burgoon, 1996). That is, the "leaner" the media, the less information a receiver has access to when attempting to make a veracity judgment on a CMC. Text-based communications, such as e-mails or online chat sessions, restrict access to visual cues and allow the receiver to analyze only the linguistic and some paralinguistic cues (Rice, 1993). "Richer" media, such as telephone or video conferencing, allow access to the majority of cues. It is within this austere computer-mediated environment that the deception detection performance of individuals' will attempt to be improved.

As discussed earlier, research has shown that training on the reliable verbal and nonverbal indicators of deception may improve a receiver's detection performance (deTurck et al., 1990; deTurck, 1991; Porter et al., 2000; Zuckerman et al., 1984). Furthermore, error detection from stored data may be improved (Klein and Goodhue, 1997). Traditional training, or "training where a time lag exists between when the training occurs and when the task to which the training is to be applied takes place,"

(Biros et al., 2002:4) based on the reliable verbal and nonverbal indicators of deception should improve deception detection performance. False alarms, or "non-deceptive data incorrectly identified as being deceptive," (Biros et al., 2002:4) occur when individuals are highly aroused or suspicious (Miller and Stiff, 1993; Parasuraman, 1984; Stiff et al., 1992). Traditional training, by its definition, allows for a time lag between when the training is given and when it is to be applied to a task. Because of this time lag, there should be less suspicion and arousal leading to a negative effect on false alarms. Thus, the following hypotheses were developed:

> H1a: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.
>
> H1b: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be negatively associated with the occurrence of false alarms.

However, according to Navarro and Schafer (2001), individuals trained in deception detection tend to lose their abilities over time if they do not practice what they have learned. Due to this suggestion, just-in-time training, or "training that occurs immediately before the target task takes place," (Biros et al., 2002:5) is likely to prove more effective than traditional training (Gilleard, 1996; Globerson and Korman, 2001; Lin and Su, 1998; Kester et al., 2001). Unfortunately, because the just-in-time training is conducted with a specific task in mind (i.e. in this case deception detection) an individual's suspicion may be aroused, thus having a positive effect on false alarms (Burgoon et al., 1994; Parasuraman, 1984; Toris and DePaulo, 1985). Thus, the following hypotheses were developed:

H2a: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.

H2b: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.

With a combination of traditional and just-in-time training, it is expected that the deception detection performance will be at the highest level, as well as the occurrence of false alarms. The logic that applies to each form of training individually should hold true for the combination. Thus, the following hypotheses were developed:

H3a: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.

H3b: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.

Figure 2 is the proposed research model for the study of training effects on deception detection performance in a computer-mediated environment. The model was adapted from Biros, George, and Zmuds' (2002) research model for inducing sensitivity to deception in order to improve decision-making performance (see Figure 2).

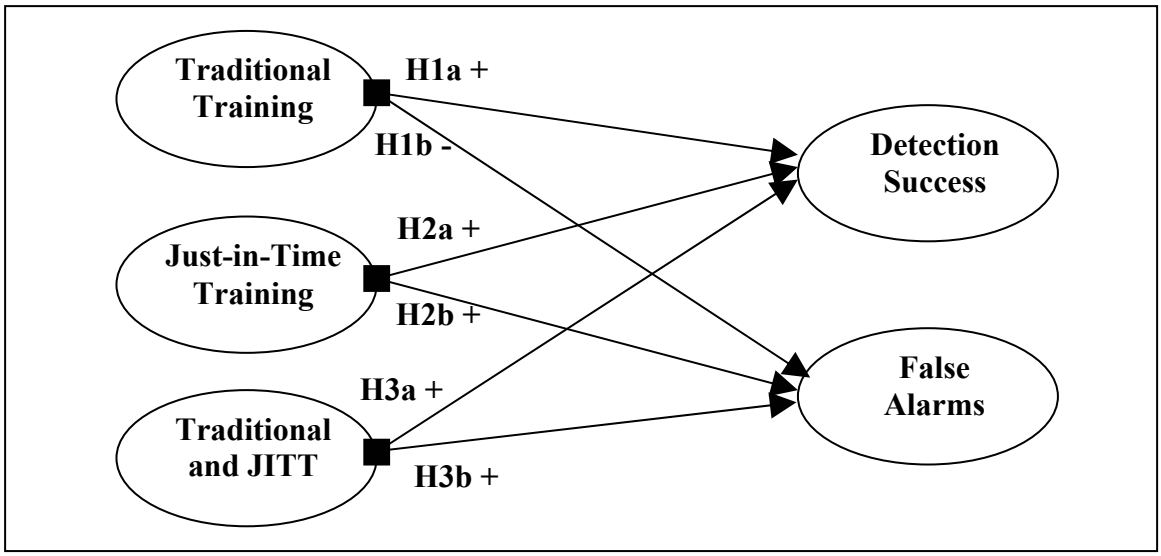

Figure 2. Proposed Research Model

Summary

This chapter discussed the theories and components that make up deception detection. CMC was defined and discussed within the realm of deception detection. A theoretical model was proposed for studying the training effects on deception detection performance in a computer-mediated environment. Both academics and practitioners benefit from understanding the theories of deception and deception detection. Researchers may use this information to increase the computer-mediated deception detection body of knowledge. Practitioners may use this information to develop automated deception detectors for installation on information systems. The forms of deception detection were explored with respect to the decision-making process and how they are an integral part of Libicki's (1995) seven forms of information warfare. Hypotheses were posited and the constructs were defined with respect to deception detection, training and the computer-mediated environment within which individuals will be trained to detect deception.

The next chapter will discuss the research methodology used to test the hypotheses suggested in this chapter. Specifically, the longitudinal experiment will be detailed and the groups that will be trained will be discussed. Chapter Four will discuss the data analysis from the longitudinal experiment. Chapter Five will discuss the research findings, any limitations that were found in the experiment, and suggestions will be made for further research.

III. Methodology

Overview

Chapter One described the research problem, provided background information, and Chapter Two discussed the current literature relevant to this thesis effort. A research model was presented, and hypotheses were derived from the proposed model. This chapter will describe the methodology used to investigate the research hypotheses proposed in Chapter Two. Furthermore, this chapter will justify the use of an experiment to test the proposed hypotheses, describe the relevant population, and provide the details of the experiment performed.

Research Methodology

In order to test the proposed hypotheses from Chapter Two, an experiment was the methodology chosen for this thesis effort. The experiment was collaboratively designed by academics working on the research project described in Chapter One. For this reason, some of the surveys and treatments in the experiment are beyond the scope of this thesis effort. The methodology description will focus on the aspects of the experiment that are related to the hypotheses of this thesis effort.

The effects of training on deception detection performance and the occurrence of false alarms are the observations (O's) of interest for this thesis effort. This means that the treatments (X's) of interest are that of deception detection training. In order to measure the significance of the proposed hypotheses, a quasi-experimental nonequivalent control group design was the methodology chosen for this thesis effort (Campbell and

Stanley, 1966). This specific design was chosen, as opposed to the true experimental pretest-posttest control group design, because the subjects were already assigned to classrooms and their training would have been interrupted by random assignment into new groups. However, the quasi-experimental nonequivalent control group design still provides sufficient control in order to minimize threats to internal validity (Campbell and Stanley, 1966). For each of the 3 sessions conducted for this thesis effort, the following setup is utilized:

Subject (Trained) Group:	**O**	**X**	**O**
Control (Untrained) Group:	**O**		**O**

From the hypotheses presented in Chapter Two, the just-in-time measurements are captured within sessions, and the traditional and combination measurements are taken between sessions.

The timeline presented in Table 1, which presents an overview of the entire experiment, reports the amount of time allotted for all of the experiment's activities. As illustrated in Table 1, the experiment was accomplished over four sessions, referred to as sessions zero, one, two, and three. There was a one-week lapse between session zero and session one, and two-week intervals between the other sessions. The only objective of session zero was to perform preliminary data collection. The next three sessions included assessing subjects' deception detection abilities and knowledge level, training subjects to detect deception, and administering other surveys.

Table 1: Research Design

Session 0	**Time(min)**	**Time(cumulative in hrs)**
AFIT Survey 0 (Demographics and others)	60	1
One week lapse		
Session 1	**Time(min)**	**Time(cumulative in hrs)**
Overview Knowledge Pretest 1a	15	.25
Judgment Accuracy Pretest 1a	15	.25
Overview Training	60	1.5
Overview Knowledge Posttest 1b	15	1.75
Judgment Accuracy Posttest 1b and Accuracy Feedback (on both tests)	15	2
AFIT Survey 1 (pertinent to other research studies)	30	2.5
Two week lapse		
Session 2	**Time(min)**	**Time(cumulative in hrs)**
Cues Knowledge Pretest 2a	15	.25
Judgment Accuracy Posttest 2a	15	.5
Cues Training via three different delivery modes (classroom, software-based, and a combination of classroom and software)	60	1.5
Cues Knowledge Posttest 2b	15	1.75
Judgment Accuracy Posttest 2b and Accuracy Feedback (on both tests)	15	2
AFIT Survey2 (pertinent to other research studies)	60	3
Two week lapse		
Session 3	**Time(min)**	**Time(cumulative in hrs)**
Heuristics Knowledge Pretest 3a	15	.25
Judgment Accuracy Pretest 3a	15	.25
Heuristics Training	60	1.5
Heuristics Knowledge Posttest 3b	15	1.75
Judgment Accuracy Posttest 3b and Accuracy Feedback (on both tests)	15	2
Debriefing and feedback	60	3

Data Collection

An Internet web site (http://en.afit.edu/env/dds) was used to collect the demographic information, as well as the knowledge and judgment assessment responses. Removing the need for the researchers to transfer the subjects' responses from a paper-based survey to an electronic format saved time and minimized the possibility of error. Furthermore, this method allowed for an organized presentation of the data, as well as immediate transfer of the responses to a database for interpretation and study.

The surveys and assessments were completed in a classroom setting with a research administrator present. The training students' were randomly assigned to one of four groups. This was necessary for one of the previously mentioned research studies that accompanied this thesis effort. At the beginning of every knowledge and judgment assessment the training student was instructed to enter their assigned group number, and four-digit identification number. The training students were tracked throughout the experiment with the combination of these two numbers, allowing for the comparison of demographic information and judgment accuracy. Instructions detailing every experimental task were produced and given to each research administrator so that consistency of the measurements and treatments was achieved between groups.

Population of Interest

The argument that deception detection is important to Air Force and Department of Defense members was discussed in Chapter One, based on the Air Force and Joint information operations objectives. According to AFMAN 26-2105, information operation activities are largely the responsibility of communication and information

personnel. Considering the Air Force is relying on the deception detection abilities of communication and information personnel to detect deception, these individuals are the population of interest for this study. The experiment was conducted on a military installation that provides training to communications personnel. This venue provided the largest possible sample (121) of communications personnel able to participate in this study. The subjects took part in the experiment as part of their daily training curriculum, and were informed the purpose of the experiment was to develop a training program for deception detection. The research administrators organized the subjects in classes based on the date they began their communications training. Eight classes, from fourteen to seventeen subjects each, were available to participate in the experiment. In order to reduce the impact of the experiment on the subjects, they remained in their previously assigned classes. The research administrators highly recommended the subjects take part in the experiment, but it was made clear that the experiment was not mandatory.

The vast majority of the subjects were Air Force officers. However, the study also included some civilian personnel and foreign officers. All the subjects had at least a bachelor's degree, and some had obtained higher levels of education. The majority of subjects reported spending over fifty percent of their workday on a computer. Most of the subjects were relatively new to the communications field, although some reported prior enlisted experience in the career field. Overall, the average amount of time in the communications field for all subjects including prior enlisted time calculated to three years. Appendix A provides a summary of the subjects' demographics. Appendix B includes a complete list of demographics questions posed. The total number of subjects who provided usable data is 119. The study began with 121 subjects; however, one

foreign officer chose to withdraw due to a language barrier, and another subject provided unusable data.

Pilot Study

The objective of the pilot study was to test the technical feasibility of the experiment, and obtain feedback on the design of the experiment and the instruments used to collect data. The pilot study included a judgment accuracy pre and posttest, a training session on the cues of deception, and several other measures of interest to other researchers. The subjects in the pilot study, nineteen volunteer Air Force Institute of Technology students, provided feedback on the readability of the instruments, the quality of the scenarios used for the judgment accuracy assessments, and the content of the lecture. In addition, the pilot study allowed for the verification of the technical feasibility of the experiment. As a result of the feedback provided, some changes were made to the presentation of the instruments. The complaints about the scenarios used for the judgment accuracy tests were mostly dealing with the audio quality, so the poor quality scenarios were removed from the experiment and replaced with higher quality scenarios. The pilot study was beneficial for resolving many unforeseen issues before conducting the experiment.

In addition to this pilot study, another institution collaborating in this research effort conducted two other pilot studies. These pilot studies were designed to test the appropriateness of the judgment assessments and the usability of the software based training program. Using data from the pilot studies the judgment accuracy tests were rated by difficulty level; this rating was used to balance the difficulty level of the pretests

with that of the posttests. These subjective difficulty ratings will be discussed in Chapter Five as part of the Limitations section. In addition, the studies returned favorable feedback on the usability of the software-based training system, Agent99.

Permission to Conduct the Experiment

Given this study involved the topic of deception, the experiment was reviewed by the Human Subjects Review board**.** An exemption to AFI 40-402 was requested and granted by the Wright Site Institutional Review Board Chairman and the Air Force Research Laboratory Chief of Aerospace Medicine**.** The exempt Protocol Request FWR 2003-0022-E authorized research involving human experimentation.

Experiment Execution

An overview of the experiment was offered earlier in the chapter and Table 1 was presented to illustrate that description. This section will review in-depth the elements of the experiment introduced in Table 1. Session zero consisted of the collection of demographic information and other data collection not of interest to this study. Sessions one, two, and three were very similar. Of the four groups in the study, three received training and one (the control group) did not. Each session began with a knowledge pretest and a detection accuracy judgment for all the groups. Then, the three groups receiving training participated in a fifty-minute training session, while the control group was released for a break. Next, all the groups took a knowledge posttest and another detection accuracy judgment; upon completion of the tests all the groups were provided with feedback on their judgment accuracy. Finally, the subjects completed surveys measuring various items of interest to other research efforts. The following sections will

provide further descriptions of the tests administered, the training provided, and exactly how the hypotheses proposed in Chapter Two were measured.

Training Treatment

The training was the treatment in this experiment. Training was provided to groups one, two, and three; group four was not exposed to any training. The session one lecture provided a broad overview of deception topics and definitions of commonly used terms. Session two training curriculum covered specific indicators, or cues, of deception, and characteristics of truthful messages. Heuristics, or mental shortcuts that people use to process information as a hindrance to deception detection, were discussed in the session three lectures. The research administrators rotated between groups throughout the experiment to prevent instructor bias. For sessions one and three, all the training was provided by a research administrator using a Microsoft PowerPoint slide show as a visual aid. Session two, however, was presented in three different formats, which will be discussed next.

Session two built on the content provided in the session one overview lecture and covered specific indicators, or cues, of deception. The session two cue training was provided via three different delivery modes in support of another research effort. The training lecture with an accompanying slide show was presented to one group. This lecture also included examples similar to the interview scenarios used for the deceptive judgment assessments, as well as military oriented examples of deception. In the first training treatment group, these examples were projected on an overhead throughout the lecture. Another group received the same content via a software-based training tool, or

Agent99. The Agent99 treatment group had access to a videotaped lecture, mirroring the lecture provided to the first training group, and the examples mentioned above. Subjects viewed the contents of Agent99 on a computer with a set of headphones. They were given complete freedom to view all of the contents, in any order, within the fifty-minute training period. The third treatment group was lectured with the same slideshow as the traditional training group; however, the examples were not played during the lecture. Rather, the subjects were given the opportunity to view the examples within the Agent99 software after the lecture was complete. Although different delivery modes were utilized, all the groups were provided with exactly the same training content. Considering all groups received the same lecture content, the delivery mode is not a concern to this thesis effort. The groups that received training will be combined and be considered the treatment group, and the group that did not receive training is the control group.

Each of the groups (including the control group) received feedback on their accuracy judgments following the judgment accuracy posttest for each session. The research administrator simply read off whether the scenarios were truthful or deceptive. No further explanations of the messages were provided; the research administrator did not elaborate on any deceptive cues the interviewee displayed or comment on what they lied about. Past research would suggest (Zuckerman et al., 1984) the feedback would have no significant impact on judgment accuracy because of the lack of content provided about the message.

Knowledge Assessments

Knowledge assessments were administered to all groups twice during each session. Communications research experts created the knowledge assessments. The assessments for each session were designed to cover the topic of interest for that particular session. The pre and posttests asked the same questions in a different order. The questions on the session one knowledge tests dealt with basic deception knowledge, such as the definition of deception and what biases prevented detectors from making accurate judgments. The session two questions were tailored to assess the subjects' knowledge concerning deceptive cues, while the session three knowledge tests evaluated the subjects' knowledge of heuristics, or mental short cuts used to process information. Appendix C contains a complete list of knowledge questions asked. The knowledge assessments were not used to calculate detection or judgment accuracy for this thesis effort. They were used to establish baseline knowledge levels for the subjects, as well as verify that the subjects were actually retaining the knowledge they received during the training treatments.

Judgment Assessments

The judgment accuracy assessments were the most important tests of the experiment; these assessments measured the subjects' judgment accuracy. The subjects were third person observers of interview scenarios. The assessments consisted of six interview scenarios in which the interview respondent was either honestly or deceptively replying to the interviewer. Each test contained three truthful and three deceptive messages presented in various media. The media levels of the scenarios were, from

highest to lowest richness level, video (with audio), audio only, or text; each test contained two questions of each media type. The order in which deceptive versus truthful messages were presented was randomly assigned, as was the order of the media richness level of each scenario.

These clips were all developed from controlled experiments designed by experts in the communications research field (Buller and Burgoon, 1994b; Burgoon et al., 1994; Burgoon et al., 1999). The video and audio clips were all in an interview format; the interviewer and interviewee roles were both filled by research participants. During the interview the interviewer asked the interviewee emotional, factual, and opinion questions and the interviewee responded to some of the questions truthfully and some deceitfully as assigned by the researchers executing the experiment. The interviews were taped from a concealed video camera for later analysis. These interviews originally included several questions, and lasted up to fifteen minutes. For the purposes of this thesis effort, the interviews were edited into clips containing only one lead question and any related questions asking for clarification or further explanation of the response. The edited clips ranged from one to three minutes in length. The clips were presented in video and audio formats, and others were presented as transcripts for the text examples. A few of the text examples were transcripts from face-to-face interviews, but the majority of text examples were transcripts from online chat interrogations. These examples were developed during a mock theft experiment where the interviewee was questioned about a missing wallet during a synchronous chat session (Research Consortium, 2001). Some of the interviewees were instructed to answer the questions deceitfully while others were not given any specific instructions. The transcripts were presented to the subjects of the

current experiment; they were given two and a half minutes to read the chat transcript and assign a veracity judgment to the scenario.

Some researchers have criticized the use of third person observers as deception detectors as outdated and unrealistic (Buller and Burgoon, 1996). However, it has also been argued that observers "offer viable perspectives on interaction," and that studying observer ratings of veracity still remains important in deception research (Burgoon et al., 1996). In this study, the third person observer role is actually quite realistic considering the interest is in deception over electronic media. The text examples used are actually chat session transcripts, which could be comparable to observing electronic mail traffic. The use of the audio example is equivalent to listening to a conference call on a speakerphone. Whereas, the use of the video examples could be equated with an employee observing a high-level executive meeting that took place over a video teleconference.

Standardized judgment test administration procedures were scripted and provided to each research administrator. The research administrators first handed out a document describing each of the six scenarios to the subjects. The research administrator would give a short introduction to each scenario (see Appendix D for an example of the document) and then project the scenario from a computer in the classroom. The video and text messages were displayed on the overhead, while the audio messages were simply played for the class over the computer's speakers. The text messages were also provided on the handout so subjects were able to read at their own pace. After each scenario was displayed the subjects were instructed to record their answers, truthful or deceptive, both on their handout and on the web site.

Hypothesis Measures

In Chapter Two a set of hypotheses was developed suggesting that traditional, just-in-time, and a combination of tradition and just-in-time training would be positively associated with deception detection success. Furthermore, traditional training would be negatively associated with the occurrence of false alarms, while just-in-time, and a combination of tradition and just-in-time training would be positively associated with the occurrence of false alarms. A false alarm, in the context of this experiment, occurs when an individual incorrectly identifies a truthful judgment scenario as deceptive.

The judgment score average for each test will be computed by dividing the number of correct judgments (i.e., successfully identifying a truthful scenario as truthful and a deceptive scenario as deceptive) by the total number of judgments for the test (for every test, six judgment scenarios are given) for each subject. The false alarm average for each test will be computed by dividing the number of false alarms by the total number of truthful judgment scenarios for the test (for every test, three truthful judgment scenarios are given) for each subject. Tables 2, 3, and 4 describe how each hypothesis will be measured.

Table 2: Hypothesis 1 Measures

Hypothesis	Measures
H1a: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	1) difference of session two pretest judgment score average and session one pretest judgment score average (2a -1a)
	2) difference of session three pretest judgment score average and session two pretest judgment score average (3a - 2a)
H1b: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be negatively associated with the occurrence of false alarms.	1) difference of session two pretest false alarm average and session one pretest false alarm average (2a - 1a)
	2) difference of session three pretest false alarm average and session two pretest false alarm average (3a - 2a)

Table 3: Hypothesis 2 Measures

Hypothesis	Measures
H2a: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	1) difference of session one posttest judgment score average and session one pretest judgment score average (1b -1a)
	2) difference of session two posttest judgment score average and session two pretest judgment score average (2b - 2a)
	3) difference of session three posttest judgment score average and session three pretest judgment score average (3b - 3a)
H2b: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.	1) difference of session one posttest false alarm average and session one pretest false alarm average (1b - 1a)
	2) difference of session two posttest false alarm average and session two pretest false alarm average (2b - 2a)
	3) difference of session three posttest false alarm average and session three pretest false alarm average (3b - 3a)

Table 4: Hypothesis 3 Measures

Hypothesis	Measures
H3a: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	1) difference of session two posttest judgment score average and session one pretest judgment score average (2b -1a)
	2) difference of session three posttest judgment score average and session two pretest judgment score average (3b - 2a)
H3b: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.	1) difference of session two posttest false alarm average and session one pretest false alarm average (2b - 1a)
	2) difference of session three posttest false alarm average and session two pretest false alarm average (3b - 2a)

Summary

This chapter described the research design and methodology used to measure the hypotheses presented in Chapter Two. The method of measuring the subjects' detection accuracy and the occurrence of false alarms was presented. In addition, the experiment activities were described in detail. The following chapter discusses the results and analysis of the data collected during the experiment. Limitations of the research, implications for the Air Force, and suggestions for further research will be discussed in Chapter Five.

IV. Data Analysis

Overview

This chapter describes the results of the experiment and details the statistical procedures used to analyze the hypotheses proposed in Chapter Two. The participation rate is discussed and a statistical description of the subjects is provided, followed by a statistical analysis of each of the hypotheses. Discussion and implications of the results will be provided in Chapter Five, as well as limitations of the study, and ideas for further research.

Description of Subjects

Although the original number of subjects expected in each class was sixteen, the number varied from class to class. The class assignments were based on the date the students were available to start training. Due to administrative problems and scheduling oversights, class sizes ranged from fourteen to seventeen students. Overall, 119 students provided usable data in session zero of the experiment. However, some of the students were not present for every session. Session two only had 117 subjects, while session three ended with a total of 115 students. This was a limitation of this thesis effort and will be further documented in Chapter Five.

The subjects were divided into four groups, as described in Chapter Three for the additional research efforts. However, only the trained groups were of interest to this research effort. To ensure equivalency between treatment groups, the scores from the first judgment accuracy tests were compared; group one had an initial detection accuracy

of 51% (standard deviation (SD) = .04), group two had an initial detection accuracy of 47% (SD = .04), and group three had a 55% average (SD = .04), no significant differences were found ($F = 1\ .11$, $p > .05$). Overall, the mean pre-training detection accuracy score of all the subjects who were to receive training was 51%. This is aligned with past research, which suggests detection accuracy is no better than chance in most cases (DePaulo et al., 1985; Zuckerman et al., 1981). However, of interest to this study is the analysis of the data in relation to the hypotheses proposed. The following sections recap the hypotheses stated in Chapter Two, present the results, and report the conclusions.

Method of Analysis

Testing Hypotheses 1a, 1b, 2a, 2b, 3a and 3b involved testing paired measures. In order to simplify this test from a multivariate analysis to a univariate analysis, a derived variable was created. The derived variable was calculated by taking the difference of the paired values (Kachigan, 1991). A Student's t-test, or simply t-test, was then performed to determine if the difference is significantly greater (or less, in the case of Hypothesis 1b) than zero ($\alpha = .05$). The results of the analyses are first discussed and then summarized within tables in each of the following sections.

Analysis of Traditional Training

Detection Success

Hypothesis 1a proposed that traditional training to detect deception in a computer-mediated environment (voice, video and data) would be positively associated with detection success. To test Hypothesis 1a, the difference between the session two pretest

(2a) and the session one pretest (1a) judgment scores of each subject was calculated. The average difference of the mean session two pretest (2a) and the session one pretest (1a) judgment scores was found to be 22% (n = 89). A t-test indicated that the difference was significantly greater than zero with a test statistic of 6.75 ($p < .0001$). However, the same test was performed on session two with contradictory results. The difference between the session three pretest (3a) and the session two pretest (2a) judgment scores of each subject was calculated. The average difference of the mean session three pretest (3a) and the session two pretest (2a) judgment scores was found to be -11% (n = 87). A t-test indicated that the difference was significantly different than zero, but directly opposite the proposed hypothesis, with a test statistic of -4.07 ($p < .0001$). In this study, subjects performed significantly better at distinguishing truth and deception after receiving traditional training for session one, but just the opposite was true for session two; thus Hypothesis 1a was supported for session one, but not for session two.

Table 5: Hypothesis 1a Analysis

Traditional Training - Detection Success					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.513	.216		
2a		.727	.188		
3a	89	.624	.192		
2a - 1a		.215	.301	6.754	< .0001
3a - 2a	87	-.111	.255	-4.066	< .0001

False Alarms

Hypothesis 1b proposed that traditional training to detect deception in a computer-mediated environment (voice, video and data) would be negatively associated with the occurrence of false alarms. To test Hypothesis 1b, the difference between the

session two pretest (2a) and the session one pretest (1a) occurrence of false alarms of each subject was calculated. The average difference of the mean session two pretest (2a) and the session one pretest (1a) occurrence of false alarms were found to be -31% (n = 89). A t-test indicated that the difference was significantly less than zero with a test statistic of -8.62 ($p < .0001$). Again, the same test was performed on session two with contradictory results. The difference between the session three pretest (3a) and the session two pretest (2a) occurrence of false alarms of each subject was calculated. The average difference of the mean session three pretest (3a) and the session two pretest (2a) occurrence of false alarms was found to be 24% (n = 87). A t-test indicated that the difference was significantly greater than zero with a test statistic of 6.90 ($p < .0001$). This test showed significant difference at correctly judging truthful communication as truthful after receiving traditional training for session one, but just the opposite was true for session two. Therefore, subjects performed significantly better at correctly judging truthful communication as truthful after receiving traditional training for session one; thus Hypothesis 1b was supported for session one. However, Hypothesis 1b was not supported for session two.

Table 6: Hypothesis 1b Analysis

Traditional Training – False Alarms					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.480	.254		
2a	89	.169	.214		
3a		.401	.262		
2a - 1a		-.310	.340	-8.624	< .0001
3a - 2a	87	.238	.321	6.899	< .0001

Summarizing Hypothesis 1, Hypothesis 1a was strongly supported for session one, but just the opposite for session two. Hypothesis 1b was strongly supported for session one, but it was just the opposite for session two. This shows that traditional training from session one had a significant positive effect on detection accuracy, but did not have a significant effect on the occurrence of false alarms. Just the opposite was true for the traditional training from session two.

Analysis of Just-in-Time Training

Detection Success

Hypothesis 2a proposed that just-in-time training to detect deception in a computer-mediated environment (voice, video and data) would be positively associated with detection success. To test Hypothesis 2a, the difference between the session one posttest (1b) and the session one pretest (1a) judgment scores of each subject was calculated. The average difference of the mean session one posttest (1b) and the session one pretest (1a) judgment scores was found to be 10% ($n = 91$). A t-test indicated that the difference was significantly greater than zero with a test statistic of 3.43 ($p < .0005$). However, the same test was performed on session two with contradictory results. The difference between the session two posttest (2b) and the session two pretest (2a) judgment scores of each subject was calculated. The average difference of the mean session two posttest (2b) and the session two pretest (2a) judgment scores was found to be -12% ($n = 89$). A t-test indicated that the difference was significantly different than zero, but directly opposite the proposed hypothesis, with a test statistic of -4.77 ($p < .0001$). In this study, subjects performed significantly better at distinguishing between

truth and deception after receiving just-in-time training for session one, but just the opposite was true for session two; thus Hypothesis 2a was supported for session one, but not for session two.

Table 7: Hypothesis 2a Analysis

Just-in-Time Training - Detection Success					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.513	.216		
1b		.615	.170		
2a	89	.727	.188		
2b		.607	.143		
3a		.624	.192		
3b		.562	.171		
1b - 1a	91	.103	.285	3.431	< .0005
2b - 2a	89	-.120	.237	-4.766	< .0001
3b - 3a		-.062	.234	-2.492	< .0073

False Alarms

Hypothesis 2b proposed that just-in-time training to detect deception in a computer-mediated environment (voice, video and data) would be positively associated with the occurrence of false alarms. To test Hypothesis 2b, the difference between the session one posttest (1b) and the session one pretest (1a) occurrence of false alarms of each subject was calculated. The average difference of the mean session one posttest (1b) and the session one pretest (1a) occurrence of false alarms were found to be -8% (n = 91). A t-test indicated that there was a significant difference to zero, but directly opposite the proposed hypothesis, with a test statistic of -2.11 ($p < .0187$). Again, the same test was performed on session two with contradictory, but more expected results. The difference between the session two posttest (2b) and the session two pretest (2a) occurrence of false alarms of each subject was calculated. The average difference of the

mean session two posttest (2b) and the session two pretest (2a) occurrence of false alarms was found to be 27% (n = 89). A t-test indicated that the difference was significantly greater than zero with a test statistic of 8.94 ($p < .0001$). This test showed significant difference at correctly judging truthful communication as truthful after receiving just-in-time training for session one, but just the opposite was true for session two. Therefore, Hypothesis 2b was not supported for session one, but it was supported for session two.

Table 8: Hypothesis 2b Analysis

Just-in-Time Training – False Alarms					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.480	.254		
1b		.396	.248		
2a	89	.169	.214		
2b		.434	.191		
3a		.401	.262		
3b		.446	.230		
1b - 1a	91	-.084	.380	-2.113	< .0187
2b - 2a	89	.266	.281	8.940	< .0001
3b - 3a		.045	.294	1.443	< .0763

Summarizing Hypothesis 2, Hypothesis 2a was strongly supported for session one, but just the opposite for session two. Hypothesis 2b was strongly opposed for session one, but it was strongly supported for session two. This shows that just-in-time training from session one had a significant positive effect on detection accuracy, but did not have a significant effect on the occurrence of false alarms. Just the opposite was true for the just-in-time training from session two.

Analysis of Combination Training

Detection Success

Hypothesis 3a proposed that combination training to detect deception in a computer-mediated environment (voice, video and data) would be positively associated with detection success. To test Hypothesis 3a, the difference between the session two posttest (2b) and the session one pretest (1a) judgment scores of each subject was calculated. The average difference of the mean session two posttest (2b) and the session one pretest (1a) judgment scores was found to be 10% (n = 89). A t-test indicated that the difference was significantly greater than zero with a test statistic of 3.57 ($p < .0003$). However, the same test was performed between sessions two and three with contradictory results. The difference between the session three posttest (3b) and the session two pretest (2a) judgment scores of each subject was calculated. The average difference of the mean session three posttest (3b) and the session two pretest (2a) judgment scores was found to be -17% (n = 87). A t-test indicated that the difference was significantly different than zero, but directly opposite the proposed hypothesis, with a test statistic of -6.77 ($p < 1.000$). In this study, subjects performed significantly better at distinguishing between truth and deception after receiving combination training between sessions one and two, but just the opposite was true between sessions two and three; thus hypothesis 3a was supported between sessions one and two, but not between sessions two and three.

Table 9: Hypothesis 3a Analysis

Combination Training - Detection Success					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.513	.216		
2a	89	.727	.188		
2b		.607	.143		
3b		.562	.171		
2b - 1a	89	.096	.252	3.571	< .0003
3b - 2a	87	-.168	.232	-6.767	< .0001

False Alarms

Hypothesis 3b proposed that combination training to detect deception in a computer-mediated environment (voice, video and data) would be positively associated with the occurrence of false alarms. To test Hypothesis 3b, the difference between the session two posttest (2b) and the session one pretest (1a) occurrence of false alarms of each subject was calculated. The average difference of the mean session two posttest (2b) and the session one pretest (1a) occurrence of false alarms were found to be -4% (n = 89). A t-test indicated that there was no significant difference to zero with a test statistic of -1.40 ($p < .0821$). However, the same test was performed between sessions two and three with statistically significant results. The difference between the session three posttest (3b) and the session two pretest (2a) occurrence of false alarms of each subject was calculated. The average difference of the mean session three posttest (3b) and the session two pretest (2a) occurrence of false alarms was found to be 28% (n = 87). A t-test indicated that the difference was significantly greater than zero with a test statistic of 9.09 ($p < .0001$). This test showed no significant difference at correctly judging truthful communication as truthful after receiving combination training between sessions one and two, but just there was a significant difference between sessions two and

three. Therefore, Hypothesis 3b was not supported between sessions one and two, but it was supported between sessions two and three.

Table 10: Hypothesis 3b Analysis

Combination Training – False Alarms					
Accuracy Scores	**n**	**Mean**	**Std Dev**	**Test Statistic**	**p value**
1a	91	.480	.254		
2a	89	.169	.214		
2b		.434	.191		
3b		.446	.230		
2b - 1a	89	-.045	.302	-1.402	< .0821
3b - 2a	87	.280	.287	9.090	< .0001

Summarizing Hypothesis 3, Hypothesis 3a was strongly supported between sessions one and two, but just the opposite between sessions two and three. Hypothesis 3b was not supported between sessions one and two, but it was strongly supported between sessions two and three. This shows that combination training between sessions one and two had a significant positive effect on detection accuracy, but did not have a significant effect on the occurrence of false alarms. Just the opposite was true for the combination training between sessions two and three.

Summary

This chapter described the analysis of the data and presented the results of the experiment. The analyses showed strong support for all aspects of detecting deception regarding session one and the combination of sessions on and two. However, exactly the opposite occurred for session two and the combination of sessions two and three. While each of the Hypotheses were strongly supported or strongly opposed between sessions, there is evidence to suggest that the training for session one and the combination of

training from sessions one and two result in detection improvement and the reduction of false alarms. Exactly the opposite occurred for session two and the combination of sessions two and three, which suggests there may have been some errors in experimentation. A discussion of these results as well as complete review of the implications, applications, and limitations of this study will be discussed in Chapter Five.

V. Conclusions and Recommendations

Overview

The focus of this research effort was to investigate how training programs impact deception detection performance and the occurrence of false alarms when attempting to detect deception. Hypotheses were developed based on past research findings and current theory, and an experiment was performed to test these hypotheses. The findings of the experiment are summarized in Table 11. This chapter will discuss the implications, limitations, and suggestions for further research related to this thesis effort.

Table 11: Summary of Findings

Hypothesis	Result
H1a: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	Partially Supported
H1b: Traditional training to detect deception in a computer-mediated environment (voice, video and data) will be negatively associated with the occurrence of false alarms.	Partially Supported
H2a: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	Partially Supported
H2b: Just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.	Partially Supported
H3a: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with detection success.	Partially Supported
H3b: The combination of traditional and just-in-time training to detect deception in a computer-mediated environment (voice, video and data) will be positively associated with the occurrence of false alarms.	Partially Supported

Discussion

Hypotheses 1a, 2a, and 3a proposed that training would have a significant positive effect on detection success. Statistical tests supported these hypotheses when the session one training treatment was utilized. Traditional and combination training, measured between sessions, as well as just-in-time training, which was measured within sessions, all suggested significant deception detection improvement where session one's training treatment was utilized. Therefore, session one's training treatment does have a positive effect on deception detection performance. However, for Hypotheses 2a and 3a, when session two or session three's training treatments were measured, there was not a significant positive effect on detection success.

Hypotheses 1b, 2b, and 3b proposed that training would be associated with the occurrence of false alarms. Specifically, Hypothesis 1b proposed that traditional training would be negatively associated with the occurrence of false alarms, and this was supported by the data analyzed in Chapter Four. Hypotheses 2b and 3b proposed that training would be positively associated with the occurrence of false alarms. However, they were supported when session two or session three's training treatments were measured, and not supported when session one's training treatment was measured. This is perplexing because Hypotheses 2a and 3a were supported when exactly the opposite happened. The following discussion of results and limitations lead to an explanation of this occurrence.

Traditional, just-in-time, and combination training all improved detection success with respect to the session one training treatment. Likewise, traditional, just-in-time, and combination training all reduced the occurrence of false alarms with respect to the

session one training treatment. This second finding was unexpected and significant. According to academics, an individual's suspicion may be aroused with training that is given right before a task is undertaken, thus having a positive effect on false alarms (Burgoon et al., 1994; Parasuraman, 1984; Toris and DePaulo, 1985). However, the exact opposite occurred with respect to the training treatments of session two and three. Just-in-time and combination training within sessions two and three did not improve detection success and was associated with the occurrence of false alarms.

Limitations

The results discussed suggest that the training treatment for session one was the best in terms of improving detection success and reducing the number of false alarms, but other factors may have influenced this phenomenon. Most notably, the fact that the experiment was longitudinal suggests that the initial training treatment would have the most impact. Simply stated, because that session was the subjects first exposure to deception detection training. Furthermore, instrumentation, or "autonomous changes in the measuring instrument," could have led to the discrepancy within session two judgment scores (Campbell and Stanley, 1966). The judgment scenarios that were used to measure the subjects' detection success and occurrence of false alarms were ranked according to their difficulty level by other researchers associated with this experiment. These rankings were subjective, and may have been erroneously skewed to have more difficult questions for the judgment posttests administered at the end of sessions two and three and easier questions at the beginning of sessions two and three.

Other limitations in the research design could have prevented an optimal investigation of detection accuracy. Miller and Stiff (1993) assert that generalizable deception research procedures should provide subjects with motivation to detect deception. It is acknowledged that this research design did not provide a sufficient means of motivation to the subjects. In addition, the experiment administrators observed that the group environment in which the experiment was conducted may have introduced a confounding effect. A more desirable arrangement would have limited the visibility of other subjects during the judgment tests to ensure facial expressions, comments, or actions of other subjects would not influence veracity decisions.

Further limitations arose because the experiment was designed to explore numerous topics, in addition to the areas of interest to this thesis effort. Feedback was given to the subjects about their detection performance, which was not part of this research effort. As well, the issuance of time-consuming surveys at the end of each session may have fatigued the subjects. Regardless of these limitations, the findings of this study are still useful to both practitioners and academics.

Implications for Practice

This study contributes to practitioners understanding of deception detection. While this study has shown that Air Force communications and information officers are not proficient at detecting deception, they may be trained to improve their deception detection performance. If the AF intends to meet the objectives of information and decision making superiority, the personnel responsible for information assurance must be able to detect deception in communications. The Air Force, and any other organization

that is concerned with detection of deception, should continue to study ways to improve the detection accuracy of its personnel.

Academic Implications and Suggestions

This study provides many implications for academics and further research. This research effort adds to the deception detection body of knowledge, especially in terms of experimenting with practitioners within the military. Military personnel were able to improve their detection performance after training, but further studies are needed. Specifically, changing the method of deception judgment scenarios from third-person observer to first-person interactive status in order to add more practitioner applicability to experimentation. Furthermore, experimentation should be conducted in the most realistic way possible, i.e., within practitioner task relevant scenarios, as opposed to contrived judgment scenarios. Finally, training must be studied further in order to identify the best way to improve detection performance.

There have been many studies that explore the effects of training on deception detection performance, but there is still no universally accepted way to improve deception detection performance. Researchers need to continue studying the best way to train people to detect deception, until there is an accepted view. Experimentation and the convergence of communications and media theoretical views offer the best road for academics to improve deception detection performance.

Conclusion

Results from this thesis effort suggest that training does improve deception detection performance, and may reduce the occurrence of false alarms. These results are

beneficial to both practitioners and academics attempting to understand deception detection and the occurrence of false alarms. Researchers should use limitations identified within this study to improve studies of deception detection.

Appendix A

Demographic Variable	**n**	**Percent Of Sample**
Gender		
Male	103	86.6%
Female	16	13.4%
	119	**100%**
Rank		
2Lt	99	83.2%
1Lt	5	4.2%
Captain	4	3.4%
Major	2	1.7%
Lieutenant Colonel	1	0.8%
Civilian	8	6.7%
	119	**100%**
Education		
Bachelor's Degree	112	94.1%
Master's Degree	6	5.1%
Doctoral Degree	1	0.8%
	119	**100%**
Age		
Average (years)	28.0	
Years in Communications Career Field		
Average (years)	3.0	

Appendix B

Demographic Information

Please select a Group

Group 1 Group 2 Group 3 Group 4

Please enter the Last 4 digits of your SSAN?

Please select your gender

Male Female

Please select your Rank

2LT 1LT CAPT MAJ LTCOL COL Enlisted Civilian

Please enter your Age in Years?

Number of years you have been in Communications career field (include prior enlisted time)?

Please select your Highest Level of Educational degree obtained?

High School Associates Bachelors Masters Doctoral

How many years have you been working with computers?

Approximate percentage of your duty day spent on a computer?

< 25% 25% - 50% 50% - 75% 75% - 100%

Approximate number of off-duty hours spent on the computer per week

None 1 – 5 6 - 10 11 – 20 > 20

How many online classes or online training courses have you taken before? Including classes taken during duty and off-duty time.

Appendix C

Introduction Knowledge Test – Session 1 ***Correct responses are in bold text

1. Studies have shown that up to _____ of all job applicants, no matter what field or position, have lied on their resumes.
    a) 10%
    b) 25%
    c) 40%
    d) 75%

2. The concept that deceivers are not able to control indicators pointing to their dishonesty is the idea behind:
    a) leakage theory
    b) interpersonal deception theory
    c) truth bias
    d) immediacy theory

3. Typically, people successfully detect deception about _____ of the time.
    a) 20%
    b) 50%
    c) 80%
    d) 90%

4. In terms of detecting deception, the downside of being suspicious is that it might lead to:
    a) less detection accuracy
    b) more false alarms
    c) more truth bias
    d) poor cognitive processing

5. A simple way to define *deception* is:
    a) a message that is inaccurate in its content and assumptions
    b) a message that is purposely used to foster a false conclusion in others
    c) a message that contradicts the beliefs of the majority of society
    d) a message that blatantly breaks the norms of a society's culture

6. Past studies of deception detection were:
    a) limited in the amount of interaction between communicators
    b) highly dynamic in nature
    c) conducted using large groups of people
    d) looked at deceptive communication of long periods of time

7. Which of the following would NOT directly lead to better detection accuracy?

a) familiarity with the communicative sender
b) experience using with the communicative medium
c) familiarity with the topic of conversation
d) experience in high-risk situations

8. The tendency for most human beings to believe other people are honest by default is known as the _____.
    a) trust bias
    b) truth bias
    c) lie bias
    d) gullibility bias

9. In response to the question "How much experience do you have driving commercial vehicles?", the dishonest response of "Yes, I have driven a dump truck" would be an example of what type of deception?
    a) fabrication
    b) concealment
    c) equivocation
    d) misconception

10. Which of the following is NOT a reliable visual indicator of deception?
    a) increased blinking
    b) smiling
    c) pupil dilation
    d) self-grooming

11. Which of the following is NOT a linguistic property?
    a) the use of pronouns
    b) submissive language
    c) temporal distancing
    d) voice pitch

12. An example of the adaptor clue would be:
    a) shuffling feet
    b) clearing the throat
    c) increased voice pitch
    d) grooming the hair

Cues Knowledge Test – Session 2

1. The theory that suggests deceivers will be unable to control all of their behavior while lying is:
    a) interpersonal deception theory
    b) indicator theory
    c) cognitive effort theory
    d) leakage theory

2. Deceivers are apt to display _____ -based cues if the consequences of having a lie detected are perceived to be severe.
    a) arousal
    b) emotion
    c) cognitive
    d) tactical

3. With regard to deception, we would expect _____ messages as more likely to be dishonest.
    a) longer
    b) shorter
    c) uninterrupted
    d) content rich

4. The type of deceptive cue known as a "leveler" refers to:
    a) a glaring lack of detail
    b) voice pitch fluctuation
    c) responding to a question with a question
    d) over-generalizing terms like "everyone"

5. If asked "Have you seen Joe's missing wallet?", a deceiver using the delay tactic of tag questions would respond with:
    a) "What are you implying?"
    b) "That's too bad for Joe, isn't it?"
    c) "Who are you to ask me such a question?"
    d) "Why should I have seen it? Of course not."

6. Which of the following would NOT be a reliable cue pointing toward deception?
    a) poor detail in a particular message
    b) non-ah nonfluencies
    c) lower voice pitch
    d) less positive emotion

7. Deceivers tend to use or switch to _____ in their messages.
    a) past tense verbiage

b) faster speaking tempo
c) more detailed explanations
d) formal names and places

8. The use of terms like "maybe, perhaps, could have" is the linguistic property known as:
    a) leveling
    b) immediacy
    c) hedging
    d) rephrasing

9. "Response latencies" refer to:
    a) stuttering during a message
    b) a pause before beginning a message
    c) an attempt to change the subject before addressing it
    d) using "uh's" and "ah's" during a message

10. Which of the following is a reasonably reliable indicator pointing toward deception?
    a) vocal pleasantness
    b) limited body movement
    c) monotone speaking
    d) unusual details

11. It is possible that a deceiver is having a difficult time lying if we notice him _____.
    a) respond immediately after being asked a question
    b) fail to maintain eye contact with others
    c) behave in a normal manner
    d) drop the names of others into conversation

12. When relating a past event, an honest communicator is less likely to:
    a) report on his or her emotional state at the time of the event
    b) report on unusual details about the event
    c) report on the verbatim discussion of those at the event
    d) leave out the names of people at the event

Heuristics Knowledge Test – Session 3

1. Heuristics refer to _____.
    - **a) mental shortcuts used to quickly judge the truthfulness of information**
    - b) highly reliable rules for judging the truthfulness of information
    - c) strategies used by deceivers to successfully lie to others
    - d) methods used for accessing information that may contradict another person's statements

2. The tendency for most human beings to perceive most incoming information as truthful is known as the _____.
    - a) trust bias
    - **b) truth bias**
    - c) plausibility bias
    - d) lie bias

3. Availability bias refers to:
    - **a) judging the reliability of an occurrence based on common, similar occurrences**
    - b) basing the validity of a statement on the reliability of its source
    - c) basing the validity of a statement on how accessible supporting information is
    - d) judging the veracity of a person on how available they make themselves to others

4. An interviewer who believes the applicants he personally interviewed more than those who did not interview the applicants:
    - a) interview bias
    - b) truth bias
    - c) lie bias
    - **d) probing bias**

5. We are more likely to believe "the painful truth" from our friends than from strangers because of the:
    - a) truth bias
    - **b) familiarity bias**
    - c) friendliness bias
    - d) framing bias

6. A person who constantly scratches his arms and generally appears nervous may trigger our _____ when judging him as untruthful.
    - a) lie bias
    - **b) nonverbal conspicuousness bias**
    - c) framing bias

d) plausibility bias

7. When an receiver incorrectly judges a truthful piece of information as being untruthful, that would be scored as a _____.
    a) hit
    b) miss
    c) false alarm
    d) correct rejection

8. Deceiving someone by submitting a false initial value for them to work from is exploiting their:
    a) framing bias
    b) anchoring & adjustment
    c) plausibility bias
    d) representativeness bias

9. The tendency to treat content that sounds believable on its face as truthful is:
    a) framing bias
    b) anchoring & adjustment
    c) plausibility bias
    d) representativeness bias

10. A person who distrusts nearly everyone upon meeting them (bordering on paranoia) is susceptible to:
    a) familiarity bias
    b) arousal bias
    c) probing bias
    d) lie bias

11. If a sixteen-year old introduces herself as a medical doctor, whether honestly or not, we might be suspicious because of:
    a) unexpectedness bias
    b) familiarity bias
    c) availability bias
    d) expert opinion bias

12. Framing bias refers to:
    a) being influenced by an initial value from which to work
    b) being influenced by the way a problem is worded
    c) being influenced by the consequences of a decision
    d) being influenced by the amount of risk involved with a problem

Appendix D

Example: Judgment Accuracy Description Handout (from Test 1a)

There are six conversations in this test. Each conversation may be a videotaped interview, an interview with only audio, or a piece of text from an online chat or a transcript of interviews. Some conversations are truthful but others are deceptive. Please carefully assess the conversations, and try to identify whether they are truthful or deceptive. You have 15 minutes to finish this test.

Question 1: This is an audio recording from an interview. The interviewer is asking the interviewee "Please describe your educational background." Please listen to the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Question 2: This is a transcript from a face-to-face interview. The interviewer (**Q**) is asking the interviewee (**A**) "What event from your childhood do you remember most fondly?" Please read the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Conversation:

Q: Uh, what event from your childhood do you remember most fondly?
A: Mm, that's a tough one, most fondly, oh, it would probably be um, the Wisconsin State Fair, I got a red and white teddy bear about this high. won it myself, no one had to win it for me.

Q: You won that by yourself, how'd you do that?
A: Throwing darts, at balloons

Q: Mmm.
A: Popping balloons

Question 3: This is a video recording from an interview. The interviewer is asking the interviewee "Please describe your current or last occupation." Please watch the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Question 4: This is an audio recording from an interview. The interviewer is asking the interviewee "How ambitious are you?" Please watch the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Question 5: This is a video recording from an interview. The interviewer is asking the interviewee "Please describe a typical day of your work." Please watch the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Question 6: This is a transcript from a face-to-face interview. The interviewer (**Q**) is asking the interviewee (**A**) "What types of people tend to rub you the wrong way?" Please read the interviewee's answer carefully, and identify whether his/her answer is truthful or deceptive.

Conversation:

Q: Um, what types of people tend to rub you the wrong way?
A: .....mm, let's see uh, there's a million types of people, uh, umm, let me think: controlling.

Q: Why?
A: People that control me.

Q: Are we talking, total control or are we talking, um, basically are you, this is just a general broad based, be, give me an example, give me a situation when you consider
A: Anyone that has control over me

Q: You're in the army, you're being controlled everyday
A: Yeah, like I said there are numerous types of those people i don't like

Q: But then you're saying that you don't like any of your superiors.
A: I just don't like people who control me.

Q: But you put up with the military, you're, as high ranked as you are.
A: Yeah, I know. But they, like you said, you asked me if they rub me the wrong way, so I, anybody, I like to be in control and when somebody has control over me, they rub me the wrong way."

Bibliography

Baltes, Boris B., Dickson, Marcus W., Sherman, Michael P., Bauer, Cara C., LaGanke, Jacqueline S. "Computer-Mediated Communication and Group Decision Making: A Meta-Analysis," *Organizational Behavior and Human Decision Processes*, 87(1):156-179 (January 2002).

Biros, David P., George, Joey F. and Zmud, Robert W. "Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study," *MIS Quarterly*, 26:1-26 (June 2002).

Buller, David B. and Burgoon, Judee K. "Deception: Strategic and Nonstrategic Communication," in *Strategic Interpersonal Communication*. Eds. Daly, J.A. and Wiemann, J.M., Hillsdale, NJ: Erlbaum (1994).

Buller, David B. and Burgoon, Judee K. "Interpersonal Deception: VII Behavioral Profiles of Falsification, Equivocation, and Concealment," *Journal of Language & Social Psychology*, 13(4): 366-396 (December 1994b).

Buller, David B. and Burgoon, Judee K. "Interpersonal Deception Theory," *Communication Theory*, 6:203-242 (August 1996).

Burgoon, Judee K. and Buller, David B. "Interpersonal Deception: III. Effects of Deceit on Perceived Communication and Nonverbal Behavior Dynamics," *Journal of Nonverbal Behavior*, 18:155-184 (Summer 1994).

Burgoon, Judee K., Buller, David B., Ebesu, Amy S., and Rockwell, Patricia A. "Interpersonal Deception V: Accuracy in Deception Detection," *Communication Monographs,* 51:303-325 (December 1994).

Burgoon, Judee K., Buller, David B., Guerrero, Laura K. and Feldman C.M. "Interpersonal Deception VI: Effects of Preinteractional and Interactional Factors on Deceiver and Observer Perceptions of Deception Success," *Communication Studies*, 45:263-280 (1994).

Burgoon, Judee K., Buller, David B. and Guerrero, Laura K. "Interpersonal Deception: IX. Effects of Social Skill and Nonverbal Communication on Deception Success and Detection Accuracy," *Journal of Language and Social Psychology*, 14:289-311 (Sept 1995).

Burgoon, Judee K., Buller, David B., Ebesu, Amy S., White, Cindy H., and Rockwell, Patricia A. "Testing Interpersonal Deception Theory: Effects of Suspicion on

Communication Behaviors and Perceptions," *Communication Theory*, 6: 243-267 (August 1996).

Burgoon, Judee K., Buller, David B., Floyd, Kory and Grandpre, Joseph. "Deceptive Realities. Sender, Receiver, and Observer Perspectives in Deceptive Conversations," *Communication Research*, 23:724-748 (December 1996).

Burgoon, Judee K., Buller, David B., White, C. H., Afifi, W. A., and Buslig, A. L. S. "The Role of Conversational Involvement in Deceptive Interpersonal Communication," *Personality and Social Psychology Bulletin*, 25: 669-685 (1999).

Burgoon, Judee K. and Floyd, Kory. "Testing For the Motivation Impairment Effect During Deceptive and Truthful Interaction," *Western Journal of Communication*, 64:243-267 (Summer 2000).

Campbell, Donald T. and Stanley, Julian C. *Experimental and Quasi-Experimental Designs for Research.* Chicago: Rand McNally College Publishing Company, 1966.

Compeau, Deborah, Higgins, Christopher A., and Huff, Sid. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study", *MIS Quarterly*, 23:145-158 (June 1999).

Daft, Richard D. and Lengel, Robert H. "Organizational Informational Requirements, Media Richness and Structural Design," *Management Science*, 32:554-571 (May 1986).

Daft, Richard D., Lengel, Robert H., and Trevino, Linda K. "Message Equivocality, Media Selection, and Manager Performance: Implications for Information Systems," *MIS Quarterly,* 11(3):355-366 (September 1987).

Dennis, Alan R. and Kinney, Susan T. "Testing Media Richness Theory in the New Media: The Effects of Cues, Feedback, and Task Equivocality," *Information Systems Research*, 9: 256-274 (September 1998).

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

Department of the Air Force. *Communications and Information Utilization Field*. AFMAN 36-2105 Attachment 21. Washington: HQ USAF, 30 April 2001.

Department of Defense. *Joint Vision 2020*. Washington DC: GPO, June 2000.

Department of Defense. *Joint Doctrine for Information Operations*. JP 3-13. Joint Chiefs

of Staff, 9 October 1998.

DePaulo, Bella M., LeMay, C.S. and Epstein, J.A. "Effects of Importance of Success and Expectations for Success on Effectiveness at Deceiving," *Personality and Social Psychological Bulletin*, 17:14-24 (1991).

DePaulo, Peter J. and DePaulo, Bella M. "Can Deception by Salespersons and Customers Be Detected Through Nonverbal Behavioral Cues?" *Journal of Applied Social Psychology*, 19:1552-1577 (1989).

deTurck, Mark A. and Miller, G.R. "Deception and Arousal: Isolating the behavioral correlates of deception," *Human Communication Research,* 12:181-201 (1985).

deTurck, Mark. A., and Miller, Gerald R. "Training Observers to Detect Deception: Effects of Self-Monitoring and Rehearsal," *Human Communication Research*, 16: 603-620 (1990).

deTurck, Mark A., Harszlak, J.J., Bodhorn, R.J. and Texter, L.A. "The Effects of Training Social Perceivers to Detect Deception from Behavioral Cues," *Communication Quarterly*, 38:189-199 (Spring 1990).

deTurck, Mark A. "Training Observers to Detect Spontaneous Deception: Effects of Gender," *Communication Reports,* 4(2):81-90 (Summer 1991).

Ebesu, Amy S. and Miller, Michael D. "Verbal and Nonverbal Behaviors as a Function of Deception Type," *Journal of Language and Social Psychology*, 13(4): 418 (1994).

Ekman, Paul. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. New York, NY: Norton, 1985.

Ekman, Paul and O'Sullivan, M. "Who Can Catch A Liar?" *American Psychologist*, 46:913-920 (Sept 1991).

Farwell, Lawrence A. and Richardson, Drew C. "Detection of FBI Agents with the Farwell MERA System: A New Paradigm for Psychophysiological Detection of Concealed Information," *Brain Wave Science,* http://brainwavescience.com/FBIRPT4.htm (7 May 1993).

Farwell, Lawrence A. "Farwell Brain Fingerprinting," *Brain Wave Science*, http://www.brainwavescience.com/GrinderReport.htm (5 Aug 1999).

Feeley, Thomas H. and deTurck, Mark A. "Global Cue Usage in Behavioral Lie Detection," *Communication Quarterly,* 43(4): 420-430 (Fall 1995).

Fogelman, Ronald R., General USAF. "Cornerstones of Information Warfare." Air

Force Pamphlet, 1-11 (1995).

George, Joey F., Biros, David P. and Burgoon, Judee K. Training plans for Deception Detection. Florida State University, Air Force Institute of Technology and the University of Arizona. (August 2002).

Gilleard, Jenni. "Delivering Training Down the Line," *Industrial and Commercial Training,* 28(7): 22-27 (1996).

Gist, Marilyn E. *The Effects of Self-Efficacy Training on Training Task Performance*. Academy of Management Proceedings, 250-254 (1986).

Globerson, Shlomo and Korman, Abe. "The Use of Just-in-Time Training in a Project Environment," *International Journal of Project Management,* 19:279-285 (2001).

Granhag, Pär Anders and Stromwall, Leif A. "Deception Detection: Interrogators' and Observers' Decoding of Consecutive Statements," *Journal of Psychology*, 135:603-620 (Nov 2001).

Grice, Paul. *Studies in the Way of Words*. Cambridge, MA: Harvard University Press (1989).

Hacker, George and Steinhardt, Laura. "Wine Industry's Propaganda Misleads Public about Drinking," *Center for Science in the Public Interest*, http://www.cspinet.org/new/wineprop.htm (2 Oct 1997).

Henahan, Sean. "Science of Lying," *Access Excellence*, www.accessexcellence.org/WN/SU/lying599.html (20 Apr 1999).

Hedlund, Jennifer, Hollenbeck, John R., and Ilgen, Daniel R. "Decision Accuracy in Computer-Mediated Versus Face-to-Face Decision-Making Teams," *Organizational Behavior and Human Decision Processes,* 76(1):30-47 (October 1998).

Jacobs, Scott, Dawson, Edwin J. and Brashers, Dale. "Information Manipulation Theory: A Replication and Assessment," *Communication Monographs*, 63:70-82 (March 1996).

Kachigan, Sam K. *Multivariate Statistical Analysis: A Conceptual Introduction*, New York, NY: Radius Press, 1991.

Kalbfleisch, Pamela J. "Accuracy in Deception Detection. A Quantitative Review." Unpublished doctoral dissertation, Michigan State University, East Lansing, MI. (1985).

Kester, Liesbeth, Kirschner, Paul A., van Merrienboer, Jeroen J.G., and Baumer, Anita. "Just-in-Time Information Presentation and the Acquisition of Complex Cognitive Skills," *Computers in Human Behavior,* 17:373-391 (2001).

Klein, Barbara D. and Goodhue, Dale L. "Can Humans Detect Errors in Data? Impact of Base Rates, Incentives, and Goals," *MIS Quarterly,* 21(2):169-195 (June 1997).

Levine, Timothy R. and McCornack, Steven A. "The Dark Side of Trust: Conceptualizing and Measuring Types of Communicative Suspicion," *Communication Quarterly*, 39:325-340 (Fall 1991).

Levine, Timothy R. and McCornack, Steven A. "Linking Love and Lies: A Formal Test of the McCornack and Parks Model of Deception Detection," *Journal of Social and Personal Relationships*, 9:143-154 (1992).

Libicki, Martin. "What Is Information Warfare," National Defense University. ACIS Paper 3 (Aug 1995).

Lin, Dyi-Yih M. and Su, Yuan-Liang. "The Effect of Time Pressure on Expert System Based Training for Emergency Management," *Behaviour & Information Technology,* 17(4): 195-202 (1998).

McCornack, Steven A. "Information Manipulation Theory," *Communication Monographs*, 59:1-16 (March 1992).

McCornack, Steven A. and Levine, Thomas R. "When Lovers Become Leery: The Relationship Between Suspicion and Accuracy in Detection Deception," *Communication Monographs*, 57:219-230 (Sept 1990).

McCornack, Steven A. and Parks, M.R. "Deception Detection and Relationship Development: The Other Side of Trust" in *Communication Yearbook 9*. Ed. Margaret L. McLaughlin, Beverly Hills, CA: Sage (1986).

Millar, Murray G. and Millar, Karen U. "The Effects of Cognitive Capacity and Suspicion on Truth Bias," *Communication Research*, 24(5):556-570 (October 1997).

Millar, Murray G. and Millar, Karen U. "The Effects of Suspicion on the Recall of Cues Used to Make Veracity Judgments," *Communication Reports*, 11:57-64 (Winter 1998).

Miller, Gerald R. and Stiff, James B. *Deceptive Communication,* Newbury Park, CA: Sage, 1993.

Muir, Bonnie M. "Trust Between Humans and Machines and the Design of Decision Aides," *International Journal of Man-Machine Studies,* 27:527-539 (1987).

Navarro, Joe and Schafer, John R. "Detecting Deception," *FBI Law Enforcement Bulletin*, 70(7) (July 2001).

Non-Smokers Rights Association. "Misleading Cigarette Marketing: The 'Light' and 'Mild' Deception," http://www.nsra-adnf.ca/english/lights (20 Aug 2002).

O'Hair, H. Dan and Cody, Michael J. "Deception," in *The Dark Side of Interpersonal Communication*. Eds. Cupach, William R. and Spitzberg, Brian H., Hillsdale, NJ: Lawrence Erlbaum Associates (1994).

Olaniran, Bolanle A. "Perceived Communication Outcomes in Computer-Mediated Communication: An Analysis of Three Systems Among New Users," *Information Processing & Management,* 31(4):525-541 (1995).

O'Sullivan, M., Ekman, Paul, and Friesen, W.V. "The Effect of Comparisons on Detecting Deceit," *Journal of Nonverbal Behavior*, 12:203-215 (1988).

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

Parasuraman, Raja. "Sustained Attention in Detection and Discrimination," in *Varieties of Attention.* 243-266. Eds. R. Parasuraman and D. R. Davies. Academic Press Inc., London, (1984).

Polygraph Clarification Services (PCS). "Determining Truth or Deception," http://home.global.co.za/~polygrph/pcs.html (1 Aug 2002).

Porter, Stephen, Woodworth, Mike, and Birt, Angela R. "Truth, Lies, and Videotape: An Investigation of the Ability of Federal Parole Officers to Detect Deception," *Law and Human Behavior,* 24(6):643-658 (2000).

Purdy, Jill M., Nye, Pete, and Balakrishnan, P.V. "The Impact of Communication Media On Negotiation Outcomes," *The International Journal of Conflict Management*, 11:162-187 (2000).

Research Consortium (University of Arizona, Michigan State University, Florida State University and the Air Force Institute of Technology). "Detecting Deception in the Military Infosphere, Research Proposal," (May 2001).

Rice, R. "Media Appropriateness: Using Social Presence Theory to Compare Traditional and New Organizational Media," *Human Communication Research,* 19:451-484 (1993).

Simon, Steven J., Grover, Varun, Teng, James T. C., and Whitcomb, Kathleen. "The Relationship of Information System Training Methods and Cognitive Ability to End-user Satisfaction, Comprehension, and Skill Transfer: A Longitudinal Field Study," *Information Systems Research,* 7(4):466-490 (December 1996).

Stiff, James B., Kim, Hyun J., and Ramesh, Closepet N. "Truth Biases and Aroused Suspicion in Relational Deception," *Communication Research*, 19(3):326-345 (June 1992).

Toris, D. and DePaulo, Bella M. "Effects of Actual Deception and Suspiciousness of Deception on Interpersonal Perceptions," *Journal of Personality and Social Psychology*, 47:1063-1073 (1985).

Truster. http://www.mil-spec-industries.com/truster/technology.htm (1998).

Zmud, Robert W. "Opportunities for Strategic Information Manipulation Through New Information Technology," in *Organizations and Communication Technology,* Eds. J. Fulk & C. Steinfield. Newbury Park, CA: Sage, 95-116 (1990).

Zuckerman, Miron, Depaulo, Bella M., Rosenthal R. "Verbal and Nonverbal Communications of Deception," *Advances in Experimental Social Psychology*, 14:1-59 (1981).

Zuckerman, Miron, Koestner, R., and Alton, A. O. "Learning to Detect Deception," *Journal of Personality and Social Psychology*, 46(3): 519-528 (March 1984).

Zuckerman, Miron and Driver, R.E. "Telling Lies: Verbal and Nonverbal Correlates of Deception," in *Nonverbal Communication: An Integrated Perspective*. 129-147. Eds. A.W. Siegman and S. Feldstein. Hillsdale, NJ: L. Erlbaum, (1985).

Vita

First Lieutenant Mark M. Lankowski graduated from John S. Fine High School in Nanticoke, Pennsylvania in June of 1995. He entered undergraduate studies at Texas Christian University in Fort Worth, Texas where he graduated with a Bachelor of Science degree in Computer Science in December of 1999. He was commissioned through the Detachment 845 AFROTC program at Texas Christian University.

His first assignment was at Beale AFB, California where he served as a Communications and Information Officer in the 9th Communications Squadron from January 2000 to July 2001. In August 2001 he entered the Graduate School of Engineering and Management, Air Force Institute of Technology. Upon graduation in March 2003, he will be assigned to the 375th Communications Squadron, Scott AFB, Illinois.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
25-03-2003	**Master's Thesis**	Jun 2002 – Mar 2003

4. TITLE AND SUBTITLE

TRAINING EFFECTS ON JUDGMENT ACCURACY IN A COMPUTER-MEDIATED ENVIRONMENT

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Lankowski, Mark M., 1st Lt, USAF

5d. PROJECT NUMBER
2002-093

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/GIR/ENV/03-10

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
AFOSR/PIF
Attn: Ms. Danielle Lindsey
801 N. Randolph St., Rm #732 DSN: 426-9562
Arlington, VA 22203-1977 e-mail: Danielle.Lindsey@afosr.af.mil

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 United States Air Force (AF) has named Information Superiority the core competency "upon which all the other core competencies rely". In order to achieve Information Superiority, deceptive communication must be minimized. According to researchers, deception occurs when communicators control the information contained in their messages to convey a meaning that departs from the truth. This research draws on Biros, George, and Zmuds' (2002) deception research model to determine if training to detect deception will improve a person's deception detection performance in a computer-mediated environment. A longitudinal experiment was conducted with AF participants (N=119) where three separate training plans were provided as the treatments, and measurements of the participants' deception detection performance were taken before and after each of the three treatments. Each measurement was taken in the form of six judgment scenarios provided through three forms of computer-mediated communication. Partial support was found for training improving deception detection performance and reducing the number of false alarms in a computer-mediated environment, based upon the first training treatment and a combination of the first and second training treatments. However, contradictory results came from the second and third training treatments. The most significant finding was that the performance of AF participants attempting to detect deception in a computer-mediated environment could be improved by a training session. Further research should explore the best training methods to improve the deception detection performance of all AF members in order to achieve the goal of Information Superiority.

15. SUBJECT TERMS

Deception Detection, Information Manipulation, Training, Computer-Mediated Environment

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			David P Biros, Lt Col, USAF (AF-CIO)
U	U	U	UU	84	19b. TELEPHONE NUMBER *(Include area code)* (703) 601-4504; e-mail: david.biros@pentagon.af.mil