ISSN 1605-2021

লোক-প্রশাসন সাময়িকী
Lok Proshason Samoeeky
সংখ্যা: ৪২/No. 42
ফাল্গুন ১৪১৩/March 2007

Information System Trust and Human-External Protection in Information Combat Environment

Dr. Mohammad Liakot Ali [1]
Md. Farid Hasan [2]

Abstract: *Now a day's military command and control (C2) center collects a massive amount of information that is both complex and contradictory. Collected information is often more than can be effectively and efficiently understood by humans. Therefore, today's decision-makers have become reliant upon information systems to filter through the information and fuse that information into a computer presentation of the battle space. The degree of reliance placed in these systems by the decision-makers suggests a significant level of trust. Trust theories and models are rich in the literature, but few have been developed for the human-computer trust relationship. A recent model of trust was found that was both broad in scope and supportive of human-computer trust theories. This model was used to explore the decision-maker's trust in information systems in a C2 environment. Given the vulnerability of information systems to information security incidents such as hacking and data manipulation, this study set out to examine if the presence of such incidents would effect the decision-makers trusting behavior. This study also examined if the use of such external safeguards, such as the Computer Emergency Response Teams (CERT) and the Network Risk Assessment Certifications, would affect the decision-maker. Two laboratory experiments were conducted using a high fidelity C2. The findings from both experiments suggest that the presence of information security incidents in a fast-paced C2 environment have no effect on the decision-makers trusting behavior. Decision makers continued to trust information systems even though information security incidents occurred.*

1.0 Introduction

In means of processing and exchanging information not only are information technologies used but also they are increasingly used and relied upon to control and operate critical functions in society. This growing trend has generated sufficient interest by researchers to examine the behavior of people who rely on these information systems [Biros, 26:2002]. Most of the current research efforts have attempted to apply human-human relationship models, such as trust, to the human-information system relationship [Muir,429:1996]. While these researchers have found some evidence to support the idea that humans trust information systems in the same way humans trust other humans,

* Associate Professor, IICT, BUET.
** Programmer, BLRI, Savar, Dhaka.

there are enough significant differences to continue this line of research. Unfortunately, this stream of research is somewhat disjoint. In fact, some trust theorists described this situation as a "conceptual morass" [Barber:1983]. While there is no one generally accepted definition of trust, there are some commonalties among these definitions. For example, trust is often defined in terms of a behavior of reliance [McKnight:1999]. Mayer, *et. al;* [Mayer, 709:1995] suggests that as a person becomes reliant (through the act of bestowing trust) on another person, the trustor becomes vulnerable to the trustee. Carrying this concept to the human-information system trust relationship, it suggests that people become vulnerable to potentially negative consequences because of their trust in these systems [Bonoma, 502:1976; Giffin,104:1967]. This vulnerability becomes even greater as society continues to rely on computer technology, not only for simple automation, but also as critical and complex information systems [DeSanctis,121:1994]. This study examines some of the variables that may influence a person's trust in information systems.

2.0 Different Information Manipulation and Information System Automation and Human Trust

Information manipulation related to different concerns perhaps the greatest threat to modern military command and control centers [Kuehl:2000]. A recent Air Force News article painted a vivid picture of this type of attack: "Imagine if you told an F-16 Fighting Falcon pilot to attack a target 550 miles away, and then learned the plane's maximum range was only 500 miles. Or suppose you ordered a C-5 to deliver cargo to an airport where the runway was too short for the plane to land" [Mayer: 2000] This example illustrates the chaos made possible by the intentional manipulation of information in a military command and control (C2) system. The model of intentionally manipulating data is not new or unique to the information age. Zmud [Zmud, 95:1990] proposed that strategic information manipulation via information artifacts could serve to influence decision-making behaviors. McCornack, *et. al;* [McCornack, 83:1996] conceptualize this as Information Manipulation Theory (IMT) and the construct of truth bias. Theories on trust can be found throughout the literature. However, the term "trust" has been either vaguely or narrowly defined. This causes difficulties for scholars who wish to study and compare trust research [Golembiewski:1975].

Primarily having interpersonal trust, a great amount of trust research deals with the advent of the computer age and with the increasing role of information systems play in society, there are a growing number of studies on the trust relationship between humans and information systems. Zuboff [Zuboff:1988] examined how people trust automation in the workplace. This research found that workers tended to either distrust the technology resulting in the lessened use of the automation or over trust in the automation resulting in problems when the automation subsequently failed. Zuboff's observations have been widely supported in empirical studies [Muir, 452:1996, Seong:1999]. Some of the most cited of these empirical studies are Muir's trust in automation experiments [Muir: 1994]. Muir had subjects perform a task on system simulators that had both manual and automated controls. The subjects either experienced random errors with the automated control, consistent errors, or no errors. Muir measured the subjects' trust in the system throughout the duration of the experiment. Muir's findings were consistent with that of Zuboff and others [Wiener, 995:1980]. She found that workers monitoring automation became complacent when the automation was perceived to perform correctly. Similarly, she found workers spent more time monitoring systems considered to be error prone and suggested that following a perceived error, a person's trust will degrade but will gradually recover over time. The findings have been supported in similar studies [Lee, 1243:1992].

3.0 Different Concepts

Observed behavior is often used by human factors researchers to measure trust, especially in the widely studied population of aircrews. In these studies, subjects participate in controlled experiments using the aid of an auto pilot system to control a simulated aircraft. The goal of the research was to study the suggestion that air crews "...have a tendency to over-rely on automation to perform tasks and make decisions for them rather than using the aids as one component of thorough monitoring and decision-making processes" [Mosier, 701:2000]. This phenomenon, which they call "automation bias" is consistent with earlier work on system trust and reliance [Muir:1996]. These studies found significant evidence that this cognitive bias (i.e. automation bias) exists and may be due to excessive reliance on these trusted systems [Mosier:2000]. The phenomenon of automation bias is consistent and similar to another theory called "truth bias" offered by McCornack. Truth bias suggests that as people develop trusted relationships with others, they tend to believe what is told to them

by the trusted person without verifying the information. Furthermore, automation bias and truth bias suggests that decision-makers who rely on and trust information systems may be susceptible to information warfare tactics like information manipulation.

4.0 Model Development and Hypotheses

The model development and hypotheses are largely based on relationships between the various constructs found in McKnight and Chervany's model of trust. However, not all of the constructs in McKnight and Chervany's model were used in this study (Figure 1). Of these constructs, dispositional trust and situational decision to trust are likely to be useful in examining the research question. As evidenced in the automation bias and truth bias studies, people will demonstrate a trusting behavior (e.g. shutting down an engine given a fire indication light) if they have a preconceived trust for that type automation (fire indication light). The construct of dispositional trust captures this facet of trust. However, it might be useful to determine if trusting computers in general is more useful to predicting trusting behavior than trusting computers in specific situations. The latter is captured in the construct of situational decision to trust. This proposed model also includes a construct called *external safeguards,* which is captured in McKnight and Chervany's construct called system trust. Finally, a construct of information warfare was included in order to study the effect of this military-unique factor on trusting behavior in a C2 environment While McKnight and Chervany [McKnight:1996] show disposition to trust and situational decision to trust as two independent constructs, it is likely that a person's disposition to trust (type A) will have some affect on their decision to trust information systems in a given situation. The reverse of this relationship may also be true. In other words, a person's decision to trust a person or object in a given situation may influence their general beliefs or attitudes about that person or object. This relationship seems likely since both attitudes are formed from some previous experience, and perhaps the same experiences [Rotter, 651:1967].

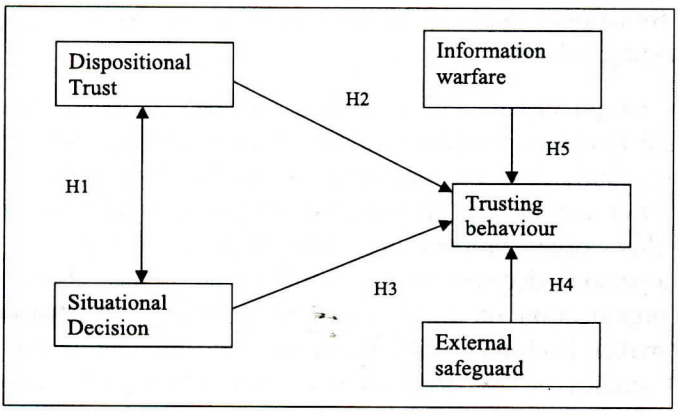

Figure 1. Adapted Model of Trust drawn from McKnight and Chervany

4.1 H1: Trust Information Systems disposition and situational decision to trust are positively correlated with each other

Dispositional trust influences a person's trusting behavior. This type of disposition to trust is often found in military battle commander's who form a general trust for the people and equipment that they work with [Boyd, 5:1992]. An example of this is a general trust in information systems to provide the necessary information for a battle commander to make a decision. This study suggests that dispositional trust will have a positive influence on a person's trusting behavior.

4.2 H2: Disposition to trust Information System positively influences trusting behavior

Studies in naturalist decision-making provide evidence that decision-making is situational in nature. The Recognition-Primed Decision (RPD) Model describes the importance of the situation with respect to forming a decision [Klein:1988]. The literature also suggests that the more positive experiences decision-makers have with objects, like information systems, the more likely they will trust the object [Mosier, 701:2000]. This phenomenon was observed in studies that examined automation bias in airline pilots. Experienced airline pilots tended to take action (i.e. trusting behavior) based solely on the information received from an automated decision support system in certain situations. Given the finding that a positive attitude or belief in a system will lead to a behavior, this study proposes that McKnight and Chervany's attitudinal construct of situational decision to trust will positively affect trusting behavior.

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

In higher tempo organizations, such as military units, personnel are conditioned to others in order accomplish their own mission objectives [Weick,361:1993] observed this behavior on the flight deck of a navy aircraft carrier and termed this behavior "collective mind." The literature supports this organizational form and mode of operation in that it suggests a person's decision to trust is influenced by the belief that some external organization or entity exists to provide a safeguard to the decision maker [Luhman:1991] However, the literature is not rich in empirical studies of this facet of trust. This study proposes that the construct of external safeguards will have a positive effect on a decision-maker's trusting behavior.

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

Much has been theorized about the effects of information warfare or strategic information manipulation on decision-makers, but little empirical research exists [Zmud, 98:1990]. What little empirical evidence does exist, suggests that the perception of information warfare events, such as computer viruses or information manipulation, will have a negative effect on decision-makers [Yeung, 8:1999].

4.5 H5: Negative effect on trusting behavior by presence of information manipulation

In summary, a person's general disposition to trust coupled with his or her situational disposition should have an influence on their trusting behavior in information systems. They should also influence each other. Further, trusting in information systems to support decision making behaviors will be positively influenced by the presence of external safeguards, but negatively influenced by an information warfare environment such as when the information system is under attack or when the system reliability has been degraded in some fashion.

5.0 Experimental Design

It was used high-fidelity computer simulator, the Distributed Dynamic Decision-making (DDD) simulator. This high-fidelity system produced a microworld within which subjects were immersed into a complex C2 computer simulation. Computer simulated microworlds offer a bridge between laboratory and field experiments by providing a realistic and

naturalistic environment and greater experimental control. While this experiment was conducted in laboratory setting, the high-fidelity DDD system closely simulates a real-world C2 decision-making environment [Entin, 292:1997]. The DDD system allowed for the collection of quantitative measures over the course of each experimental trial, as well as measurable attitudes and beliefs through a pre and post survey questionnaire. Two experiments were developed to test the hypotheses using the DDD system. Before the experiments commenced, a pilot study using 10 graduate students at a university in the mid western US was accomplished to insure the methodology was sound.

5.1 Experiment 1

In experiment1 sample size n=56. The ages of subjects ranged from 19 to 46 years old and their experience ranged from 0 to 50 hours of combat C2 experience. The typical duties of the respondents were very similar to the tasks required in the experiment using the DDD. Each subject experienced only one of the four possible conditions. Each subject was given training on the weapon system concept and computer interface. Following training, each subject was tasked by the experiment administrator to perform a hidden-profile, decision-making task that involved the control of multiple Unmanned Combat Aerial Vehicles (UCAV's) to defend one of four air space zones on a computer display. Control of each UCAV was performed through various user actions on the DDD system. The UCAV system was described to the subjects as a new operational command and control system being field tested by the research laboratories. The participants were tasked to identify incoming air tracks by electronically directing UCAVs to move within sensor range. Air tracks are a computer representation of an aircraft radar signature displayed on the participant's computer display. If the air track was identified as a hostile, they were authorized to attack the target without the need for further verification. They were told the objective of their mission was to stop all hostile tracks before they entered protected airspace. The participants were told that the UCAV computer system could automatically determine the identity of any air track once it was within the UCAV's sensor range. They were also told the computer system was 100 percent accurate in both algorithmic and display processing. The participants were cautioned that information from the UCAV aircraft and the computer system traveled across an unclassified local area network (LAN) and was therefore vulnerable to Information Warfare attacks. They were further cautioned that the simulation might

contain a simulated IW attack against the LAN. The participants were given a means to communicate electronically to verify the identity of air tracks, once the air tracks had been identified by their UCAV. Five minutes into the simulation all participants received a threat message from a simulated network participant; the Network Security Force (NSF) that indicated an attempted attack against the network had occurred. During training, the participants were told the role of the NSF was to monitor and protect the networks in the region against IW attacks. Two new tracks appeared approximately 10 seconds following the message from the NSF. For treatment groups three and four, one of these tracks appeared as a friendly when in fact it was a hostile. The other track appeared as a hostile when it was actually a friendly. If the subjects destroyed the friendly aircraft, a visual and audible alarm was triggered indicating a fratricide had occurred. In addition, subjects could perceive this error by observing a decrement to their defensive score. The first experiment manipulation was the construct called *external safeguards*. It was operationalzed in the form of a simulated game participant called the Network Security Force (NSF). The NSF was described as an external agency that was not actually part of the UCAV system. Subjects were told that the NSF's role was to monitor and protect the LAN against IW attacks. The NSF was, in essence, an external safeguard that contributed to the subject's sense of normality and confidence by providing alerts to the subjects of IW attacks. Treatment groups one and four were told by the experiment facilitator that the NSF was very effective (90%) at detecting enemy information attacks and defending the network against these attacks. Treatment groups two and three were told by the experiment facilitator that the NSF was not very effective (60%) in the same tasks. The second manipulation, Information Warfare (IW), was operationalized in the form of an information manipulation resulting in two *spoofing* events. Spoofing is a tactic whereby the enemy has covertly gained access to the system and manipulates the track identity, such that a friendly aircraft appears on the display as an enemy and an enemy aircraft appears on the display as a friendly. Treatment groups three and four were subject to an information manipulation event during the simulation, while treatment groups one and two were not. The effectiveness of the manipulations was measured by two different methods. The effectiveness of the External Safeguard manipulation was checked by a post-training multiple-choice test. Three questions on this test measured different aspects of the External Safeguard entity in this experiment, the Network Security Forces (NSF). The effectiveness of the Information Warfare manipulation was measured both by the post-test

multiple-choice test referred to above, as well as counting the number of spoofing acknowledgment messages sent by subjects who experienced the manipulation. Cognitive phenomena like attitudes, motivations, expectations, intentions, and preferences can be difficult to observe. Therefore, a survey consisting item clusters that measured these attitudes was developed and administered before and after each experimental trial. The item clusters were and adapted from self-reporting measurements developed by McKnight and others to assess the subject's attitudes and beliefs. Dispositional trust and situational decision to trust were operationalized and measured through the use of a survey that employed a cluster of items using a five-point Likert-like scale. A factor analysis was performed to derive a correlation matrix and ensure the items loaded on the predicted number of factors. In addition, a reliability analysis was performed to derive reliability coefficient alpha for the items. The reliability analysis produced an <> = .72. This reliability level is sufficient for this type of study [Nunally:1994]. Trusting behavior was operationalized in terms of the user's action or inaction based on information received from the UCAV system. In this case, trusting behavior was measured by examining how many times the user requested identification verification from an external source before taking an action or inaction. Therefore, the act of expending solely on the UCAV system is an indicator and measure of trusting behavior. Analysis and Results (Experiment 1) Hypothesis H1 predicted a positive correlation between disposition to trust and situational decision to trust. A review of the correlation analysis shows a significant positive correlation (.372) between disposition to trust and situational decision to trust at a significance level of $p < 0.001$. This finding supports Hypothesis 1 and suggests that if decision-makers trust computers in general, they will also tend to trust computers in a command and control or other high tempo environment. Hypothesis H2 predicted disposition to trust would have a positive effect on trusting behavior. The results from the regression analysis do not show disposition to trust to be significant ($p = .401$, ®= -. 574) at the 0.05 level. This finding does not support Hypothesis 2 which suggests that a decision maker's trust of computers in general is a useful predictor of their willingness to trust information presented to them on a C2 information system. Hypothesis H3 predicted situational decision to trust would have a positive effect on trusting behavior. The results from the regression analysis above show situational decision to trust to be marginally significant ($p = .069$, ®= -1.084). This finding supports Hypothesis 3 which suggests that a military commander's trust in computers in a C2 environment is a useful predictor of their willingness

to trust information presented on a C2 information system. Hypothesis H4 predicted external safeguards would have a positive effect on trusting behavior. The results from the regression analysis show external safeguards to be significant (p = .881, ®= .127). Therefore, these findings offer no support for Hypothesis 4 which suggests a decision maker's belief in the effectiveness of an external safeguard to a C2 information system would have a positive effect on their willingness to trust information presented on the C2 information system. Hypothesis H5 predicted information warfare would have a negative effect on trusting behavior. The results from the regression analysis show information warfare not significant (p = .882, ®= -9.455. Therefore, there is no evidence to support that the perceived presence of an information warfare attack has a negative effect on a decision maker's willingness to trust the information received from an information system. Discussions with some of the participants following the experiment indicate that they were so busy concentrating on performing the required tasks that they either did not have time to contact for verification or had forgotten about the option to contact. This perceived high task load may have resulted in the low number of contacts made with them. This is consistent with Biros and Daly's finding regarding task load and system trust. Therefore, a second experiment was designed to validate the findings from the first experiment and eliminate possible problems with task load.

5.2 Experiment 2

A similar command and control (C2) scenario was developed for use with the same high-definition simulator for easier comparison of results between the two experiments. This experiment collected quantitative measures of subject behaviors over the course of each experimental trial, as did the computer simulator used in the first experiment. This was done in order to allow for measurable attitudes and beliefs through a pre and post survey questionnaire in the same basic fashion as the first experiment. This experiment maintained the same between group design as the first experiment in which the same two independent variables were manipulated. Each participant was given training on the simulator and computer interface. Following training, each subject was tasked by the experiment administrator (acting as a military laboratory field evaluator and reading from a script) to perform a hidden-profile, decision-making task that involved the control of multiple fixed Surface-to-Air Missiles (SAM). Control of each SAM site was performed through various user actions on the DDD system. Subjects were tasked to identify incoming air

tracks by comparing the icon information from the graphical display with a list of automated electronic messages sent by the radar sites. If the air track was identified and confirmed by the subject as a hostile, they were authorized to attack the target using one of their SAM sites. Subjects were told the objective of their mission was to stop all hostile tracks before they entered protected airspace. Subjects were further told that the while the computer system would automatically determine the identity of all air tracks, it was possible for the automated messages sent to the computer system to be manipulated by the enemy. The number of tasks required to perform their mission were substantially reduced in this experiment in order to reduce the potential problem of task saturation observed in the first experiment. Unlike the first experiment where the IW threat and network defender were simulated, the experiment administrator introduced two people to the participants. This was done following the introduction part of the training. The participants were told these two people would be playing the role of the network attacker and the other as network defender. The participants were then told these individuals would be located in the next room where they would perform their tasks. The experiment administrator instructed the participants that they should expect to receive electronic messages from the network defender if he or she detected a network attack by the attacker. In actuality, both of these people were portraying the role of subjects. Following this explanation, these two people left the room and performed no further part in the experiment. Also unlike the first experiment, subjects were not given a means to contact another party in order to confirm the identity of the tracks. Due to the problems identified in the last experiment with this measure (i.e. the measure resulted in only one or two states: contacted or not contracted), a more robust and descriptive measure was developed for this experiment. This new measure was accomplished by requiring subjects to set a confidence level for each hostile track before initiating an attack. The confidence level was a scale from 1 to 5, where 1 represented very low confidence in the track identity and 5 represented very high confidence in the track identity. This confidence level was also tied to the scoring system so that points were calculated as a function of confidence level. Another group of sampling size 38 were selected the ages of subjects ranged from 24 to 56 years old. The experiment manipulations were the same as in the first experiment. The participants were told that the NSF's role was to monitor and protect the LAN against IW attacks. The NSF was, in essence, an external safeguard that contributed to the participant's sense of normality and confidence by

providing alerts to the subjects of IW attacks. Treatment groups one and four were told by the experiment facilitator that the NSF was very effective (97%) in detecting enemy information attacks and defending the network. The second manipulation, IW, was operationalized in the form of an information manipulation resulting in spoofing events as in the first experiment. The number of spoofing events was increased from the two in the first experiment to four in the second experiment in order to strengthen this manipulation. The IW manipulation required the user to perceive an IW attack. To achieve the perception of the IW manipulation, the DDD software was modified so that if a user attacked a friendly aircraft (to include a friendly aircraft spoofed as an enemy aircraft) an audible alarm would sound followed immediately by a pop-up window that displayed a warning message. A mouse click action was required to end the audible signal and close the pop-up window. The act of canceling this signal was used as an indication that the user perceived the IW spoofing manipulation. When the experiment was complete, subjects were given a survey and multiple-choice quiz similar to those in the first experiment. The survey, again, served as a manipulation check to ensure the subjects did indeed know they were under an information attack.

5.3 Results and Analysis (Experiment 2)

A regression analysis was conducted using the same predictors as in the first experiment: Constant, disposition to trust (DT), situational decision to trust (SDT), information warfare (IW), and external safeguard (ES). However, the dependent variable used in this model was the confidence level assigned to each air track by the subject prior to making a decision (i.e. trusting behavior). The results from the regression analysis show the model to be significant at the .05 level (df=4, F=2.788, p=0.042). Hypothesis H1 predicted a positive correlation between disposition to trust and situational decision to trust. A review of the correlation analysis shows a significant positive correlation (.603) at a significance level of $p < 0.001$ level (1-tailed) between a subject's disposition to trust computers in and their situational decision to trust computers in a specific situation. Hypothesis H2 predicted disposition to trust would have a positive effect on trusting behavior. The results from the regression analysis represent disposition to trust to not be significant ($p = .761$, ®= .060) at the 0.05 level of significance. This finding does not support Hypothesis 2 and suggests that a decision maker's trust of computers in general is a useful predictor of their willingness to trust information presented to them on a C2 information system. Hypothesis H3 predicted situational decision to trust would have a positive effect on trusting behavior. The results from

the regression analysis above show situational decision to trust to be marginally significant (p = .076, ®= .353). This finding supports Hypothesis 3 and suggests that a decision maker's trust in computers in a C2 environment is a useful predictor of their willingness to trust information presented to them on a C2 information system. Hypothesis H4 predicted external safeguards would have a positive effect on trusting behavior. The results from the regression analysis show external safeguards to be marginally significant (p = .077, ®= -.282). However, the beta coefficient is the opposite from what was predicted in Hypothesis 4. That is to say, while there is no evidence to support the hypothesis that a decision maker's belief in the effectiveness of an external safeguard is a useful predictor of their willingness to trust information presented to them on a C2 information system, there does appear to be some suggestion that the opposite may be true. Hypothesis H5 predicted information warfare would have a negative effect on trusting behavior. The results from the regression analysis represent information warfare not to be significant (p = .965, ®= .007. Therefore, there is no evidence to support Hypothesis 5 which suggests that the perceived presence of an information warfare attack, such as the manipulation of air track data, has a negative effect on a decision maker's willingness to trust the information received from a information system.

6.0 Discussion

The question of research for this study was what affect external safeguards has on human- information systems trust in an information warfare domain. It was found that dispositional trust and situational trust were well correlated with each other. However, no evidence was found to suggest that external safeguards or an information warfare environment had any influence on the participants trusting behavior. Post experiment interviews suggested that participants were so involved in the task domain that they lost focus of the external safeguards and IW present in the experiment. This task saturation seem so influential that a second experiment was designed to mitigate its effects. It also employed the command and control simulator. However, rather than use a three-dimensional aircraft tracking simulation, the second experiment used a 2 dimensional surf-to-air missile (SAM) simulation. This served to reduce the task load on the participants. Like the first experiment, the second found support for hypothesis 1, and it found support that disposition to trust will have a positive influence on trusting behavior. As with the first experiment, no support was found to suggest that the presence of external

safeguard would have a positive affect on participants trusting behavior. Further, no support was found to suggest that an IW environment (i.e. computer attack) would have a negative influence on trusting behavior.

7.0 Conclusion

The findings from these experiments suggests that humans place a great amount of trust in the information systems they use to support their decision making in high tempo situations. In the presence of dangerous situations such as information warfare environment, as evidenced by the two experiments presented, human information systems users tend to focus on the tasks they need to accomplish and fail to consider the consequences of doing so. Further, when external safeguards such as computer security entities and back up systems are available, the participants in these studies continued to rely in their primary information systems and did not use the available external safeguards. This research highlights the vulnerability to deception faced by decision-makers who rely on information systems. While it is thought the external safeguards and warnings of possible computer attack would affect decision maker's trusting behavior toward the information systems they use, the finding from the two experiments conducted for this research do not support that thinking. Further, this study serves to underscore the importance of continued research in system security and reliability.

References

Barber, B. (1983) The Logic and Limits of Trust. NewBrunswick, NJ: Rutgers University Press.

Biros, D., George, J., and Zmud, R., (2002) "Inducing Sensitivity to Deception in order to Improve Deception Detection and Task Accuracy," MIS Quarterly, 26 (2).

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

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

Burgoon, J.K., Buller, D.B., Ebesu, A.S., and Rockwell, P. (1994) "Interpersonal deception: V. Accuracy in deception detection." Communication Monographs, 61, 303-325.

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

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

Giffin, K. (1967) "The Contribution of Studies of Source Credibility to a Theory of Interpersonal Trust in the Communication Process." Psychological Bulletin, 68(2): 104-120.

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

Klein, G. A. (1988) "Naturalistic models of C3 decision making." in Science of Command and Control: Coping with Uncertainty Ed. Johnson S. and Levis A. Washington, DC: AFCEA International Press.

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

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

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

Mayer, D., (21 June 2000) "Keeping Air Force secrets secret," AirForce News.

http://www.af.mil/news/Jun2000/n20000621_000943.html.

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

McCornack, S.A., Levine, T.R., Morrison K, and Lapinski, M. (1996) "Speaking of Information Manipulation: A Critical Rejoinder," Communication Monographs, 63(1): 83.

McKnight, D. H. and Chervany N.L., (Oct 1999) "The Meanings of Trust." Research working paper, web page. http://www.misrc.umn.edu/wpaper/wp96-04.htm.

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

Muir, B. M. (1994) "Trust in automation: Part I. Theoretical issues in the study of trust and human intervention in automated systems," Ergonomics, 37(3): 1905-1922.

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

Nunally, J.C. and Bernstein, I.H., (1994) Psychometric Theory. New York: McGraw Hill Company.

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

Seong, Y., Llinas, J., Drury C.G, and Bisantz, A.M., (1999) "Human Trust in Aided Adversarial Decision-Making Systems," in Automation Technology and Human Performance. Ed. Scerbo, M. W. and Mahwah, M.M., NJ: Lawrence Erlbaum Associates.

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

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

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

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

Yeung, L. N. T., Levine, T.R., and Nishiyama, K., (1999) "Information Manipulation Theory and Communications Reports, 12(1): 1-11.

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

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