SUSPICION MODELING IN SUPPORT OF CYBER-INFLUENCE OPERATIONS/TACTICS

THESIS

Henry G. Paguirigan
Captain, USAF

AFIT/GIR/ENV/08-M17

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

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

AFIT/GIR/ENV/08-M17

SUSPICION MODELING IN SUPPORT OF CYBER-INFLUENCE OPERATIONS/TACTICS

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 Resources Management

Henry G. Paguirigan, BSOE

Captain, USAF

March 2008

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED

AFIT/GIR/ENV/08-M17

SUSPICION MODELING IN SUPPORT OF CYBER-INFLUENCE OPERATIONS/TACTICS

Henry G. Paguirigan

Captain, USAF

Approved:

//SIGNED//	21 Mar 08
Jason M. Turner, Maj, USAF, PhD (Chairman)	Date
//SIGNED//	18 Mar 08
Michael R. Grimaila, PhD (Member)	Date

Abstract

Understanding the cognitive process of *IT user suspicion* may assist organizations in development of network protection plans, personnel training, and tools necessary to identify and mitigate nefarious intrusions of IT systems. Exploration of a conceptual common ground between pycho-social and technology-related concepts of suspicion are the heart of this investigation. The complexities involved in merging these perspectives led to the overall research question: *What is the nature of user suspicion toward IT*? The research *problem/phenomenon* was addressed via extensive literature review, and use of the Interactive Qualitative Analysis methodology. A focus group consisting of military IT professionals identified their representative system of the problem/phenomenon. Analysis of the system led to the development of a model of IT suspicion as a progenitor for future experimental constructs that measure or assess behavior as a result of cyber attacks.

Acknowledgments

I am very grateful for the education I received here at AFIT, especially the learning experience of producing a graduate level thesis. I wish to thank my education advisor and thesis committee member, Doctor Michael R. Grimaila, for his assistance in initiating this process and for the words of encouragement. I am especially grateful to my thesis advisor and committee chair, Major Jason M. Turner for his invaluable time, comments and personal attention in support of this thesis effort. I express my sincere appreciation for his mentorship, leadership and work ethic which I have embraced as part of my own cathexis. I was so fortunate to have him as my thesis advisor and AFIT should be so privileged to him as part of their faculty.

I also owe my thanks to my IRM colleagues and friends who in the course of our studies were ardent supporters of each other, with diverse personalities that added levity during my coursework. I am also indebted to those colleagues who participated in my focus group – thanks for providing their "mindmap." Finally, my most heartfelt thanks go to my wife for her patience and infinite support throughout this endeavor. Her love and devotion to our family over the years; placing her own aspirations on hold to further my achievements, have translated into success for our family; hence, I express my deepest gratitude and appreciation.

Henry G. Paguirigan

Table of Contents

Page

Page

Page

List of Figures

Page

List of Tables

Page

SUSPICION MODELING IN SUPPORT OF CYBER-INFLUENCE OPERATIONS/TACTICS

CHAPTER 1: INTRODUCTION

Background

Technological advances such as the personal computer and Internet have revolutionized the way people communicate and have enabled users to swiftly and reliably transmit large amounts of information worldwide. The diffusion of these and other related technologies has been embraced, to a large extent, by the global community. The more generalized term "information technology" (IT) has come to describe the various incarnations of such technological advances and includes "any communications device or computer, its ancillary equipment, software applications, and related supporting resources" (AFDD 2-5, 2005, p. 52). IT is used increasingly for academic, business, personal, government, and military purposes. In effect, IT has become a common tool in everyday life for users in rich and poor countries alike (The Economist, 2007).

This global proliferation of IT has increased the number of interactions between humans and technology. According to Bonito, Burgoon, Bengtsson (1999), interpersonal interactions are subject to certain expectations that a person confers on the other. For example each member of a group is expected to make useful (positive) contributions toward a group goal; however, members of a group can also expect extraneous (negative) contributions toward a group goal from other group members. These expectations influence the nature of the social interaction as each member forms impressions on other members. A negative impression may influence a member to question another member's

ability to contribute toward a task; hence affecting a member's decision to trust the other. The role of expectations in human-to-technology interactions is equally as valuable as such expectations provide a basis for evaluation of task accomplishment and behavior of the technology. We expect our technology to be dependable and secure, which provides us the ability to know how a technology will behave (Flechais, Riegelsberger, and Sasse, 2006). A perceived violation of such expectations may arouse suspicion…suspicion which might prompt a person to reevaluate the interaction or the technology itself – leading to a decision to trust or distrust the technology. Given the notoriety and popularization of notions such as hacker attacks or identity theft, it is reasonable to conclude that many people have good reason to be suspicious of technology. Yet despite the potential for such suspicions, modern life is marked by an ever-increasing dependence on IT, even in the military.

The criticality of IT is especially evident in the DoD's transformation into a "network-centric" force – a force using network, information, and Internet-like technologies to allow users to create and share information anywhere in the operational battlespace (DoD CIO, 2005). The US military's current approach toward such transformation is to exploit IT as an enabler for the strategic success of current and future operations and to gain *information superiority*. 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" (JV 2020, 2000, p. 8). For example, today's military missions rely heavily on information for joint operations. Such operations require the rapid collection of information, which, when converted to useful knowledge, translates into superior battlespace awareness and better

and faster decisions by commanders. IT allows the military (as well as other organizations) to share, transmit, or store information, and integrate that information into the decision-making process in an accurate and timely manner.

The significance of this integration and achieving information superiority is to ensure a definitive competitive advantage of the military over its adversaries. This competitive advantage manifests itself in the form of *decision superiority*. Joint Vision 2020 (2000) describes decision superiority as the critical ability of the military to take advantage of information and convert it to superior knowledge. Air Force Doctrine Document 2-5 (2005) also defines decision superiority in terms of "…improving our ability to observe, orient, decide, and act (the OODA loop) faster and more effectively than the adversary" (p. 1). The key to effectively managing the OODA loop is in realizing that whoever progresses through this cycle more swiftly and acts more rapidly than the adversary can "get inside" the opponent's decision cycle to gain a military advantage (Gibb, 2000).

The information environment is one in which humans and information technologies interact regularly; the OODA loop is also executed within this environment as a primary means of decision making (JP 3-13, 2006). The information environment consists of three dimensions: cognitive, information, and physical. Of these three dimensions, the cognitive dimension is the area in which people think, perceive, visualize, and decide, "…it is the most important of the three dimensions" (JP 3-13, 2006, p. I-2). It is also the dimension in which suspicion of IT plays a critical role, for while technological advancements and IT enable the exchange of vast amounts of information,

perceptions of that IT may affect how successfully the information shared, transmitted, or stored using IT is ultimately applied to our decision making process.

For instance, suspicion arousal may hamper the fluidity of a military operation by creating an obstacle as a result of acting on the perceived suspicion. For example, a commander who becomes too suspicious to act on IT-founded intelligence, may end up wasting valuable time getting HUMINT to confirm what sensor data had already suggested was true). Thus, a potential conflict has developed between the military's reliance upon IT and the ways in which potential suspicion of IT could mitigate how effectively such technologies can be used to enable military operations.

Regrettably, the more the military relies on IT as an enabler for its operations and decisions, the more vulnerable our operations and decision-making abilities may become. For example, our adversaries have long recognized the US military's reliance on information technology (Hebert, 2005). Thus, the perceived advantage IT confers on the US military can also be a source of potential disadvantage as emerging technologies introduces new vulnerabilities (AFDD 2-5, 2005). For this reason, information security has become critical to military operations and the integrity of the OODA loop. Information security is "The protection of information and information systems against unauthorized access or modification, whether in storage, processing, or transit, and against denial of service to authorized users" (JP 3-13, 2006, p. GL-9).

Information security vulnerabilities are those information systems and resources that are susceptible to attacks from adversaries. For example in 1997, an NSA-led team of hackers launched a successful attack on supposedly secure Pentagon computer networks (Hebert, 2005). What was extremely disturbing about this attack is the fact that publicly

available computer equipment and hacking software were used to infiltrate and take over several US Pacific Command computers and emergency systems in major cities.

Many of the details of the NSA-led exercise, code-named "Eligible Receiver," are still classified; however, this in-house exercise highlights what may be very real examples of our adversaries' capabilities. Indeed, there have been numerous attempts to access US technology and information, a third of which were traced to foreign entities (US GAO, 2004). For example, hackers traced to servers in China had inserted a virus into the US Department of Commerce's information system. This attack resulted in the replacement of hundreds of computers resulting in costly repairs and loss of productivity (Roberts, 2006). The Air Force Personnel Center was also successfully attacked by an unidentified perpetrator who hacked into the Assignment Management System database and retrieved names, birth dates, and social security numbers of over 30,000 personnel, hence making many in the Air Force potential targets for identity theft (Hebert, 2005).

Clearly, the military's reliance on IT creates a number of potential vectors for attack that could be costly in terms of money, mission accomplishment, even lives. With that in mind, it is imperative that military personnel remain vigilant, especially those, such as computer users, who are in direct contact with the technologies used to access and manipulate elements of the information environment. In this sense, the notion of suspicion in IT may actually serve as a source of strategic advantage because the vigilance required to help guard against IT-based attacks and ensure a degree of information security may also have its roots in IT suspicion-related issues. For example, a person generally suspicious of IT while using a computer may be more likely to act on a

perceived suspicion and detect a potentially harmful deceptive adversarial operation than a person who is not generally suspicious of IT.

Research Focus

As the reliance on IT in the military increases, so do the vulnerabilities and threats. As USAF Lt. Gen. C. Robert Kehler, STRATCOM's Deputy Commander, recently said, "The more the military comes to rely on network-based operations, the more it must defend those networks" (Hebert, 2005, p. 65). However, there are important processes happening in the minds of IT users that could mitigate network attacks, or at least make IT users more sensitive to such attacks when they happen. Such processes occur in the cognitive dimension of the information environment – a realm that has primarily been studied and associated with the field of psychology (Hebert, 2005). As such, the cognitive dimension is the dimension in which people think, perceive, visualize, and decide (JP 3-13, 2006). One such process occurring within this dimension is that of suspicion – a process that may be key to alerting users of potential attacks or compromises in the IT-based elements of the information environment.

The notion of *suspicion towards IT* per se has not received a great deal of direct attention and study, at least not enough to provide an explicit definition and conceptual model that would be useful within military operational or training contexts. Specifically, the existing research on suspicion has been predominantly conceptualized only in terms of interpersonal relationships and social interactions. Within the technology-related literatures, there are relatively few discussions of suspicion; however, there are discussions of similar or related concepts such as trust and deception detection. The need

to establish some conceptually common ground between these many perspectives is at the heart of the current investigation. Indeed, as Grabner-Kräuter, Kaluscha, and Fladnitzer (2006) note, "In order to make progress in a scientific field, scholars need to find a consistent terminology to be able to adequately test their hypotheses, to communicate their results among each other and to build on each others findings" (pg. 1).

With this notion of consistent terminology in mind, the existing literature's treatment of user suspicion toward IT using associated or related concepts may be missing something fundamental, or at least something that stands in the way of enabling progress due to the lack of a consistent definition and conceptualization of suspicion towards IT. Perhaps such a definition might even be informed by the aforementioned research and focus on the interpersonal aspects of suspicion. For this reason, a consideration of both the interpersonal and technology-related literature streams and perspectives on suspicion and suspicion-related constructs seems appropriate for developing a better understanding of what suspicion towards IT is (or might be). Therefore, relevant literature streams from both psycho-social and IT-related fields of study will be presented in the following sections such that it becomes clear that suspicion towards IT may be more complex than previously thought (or modeled). It is these complexities that are of interest throughout the remainder of this study and ultimately inform the overall research question at the heart of this investigation: *What is the nature of user suspicion toward IT?*

Research Impact

The results of this study may provide a framework for others to build upon; possibly for the creation of an IT suspicion-model which could be acted upon by any organization that must protect its information technologies and systems from adversarial attack. A suspicion-modeling system could also be beneficial for the detection of technology-based deception (DeRosis, Castelfranchi, Carofiglio, 2000); specifically helping to train IT users to detect such deception, as well as helping to develop the tools necessary to identify and thwart information technology and systems attacks. From an offensive standpoint, a better understanding of IT suspicion could facilitate the development of IW attack tools and strategies. For instance, imagine if IW attacks were conducted such that they did not raise adversarial suspicion, or at least raise that suspicion to a level high enough to prompt an adversary to take action and ultimately thwart an IW operation? The following chapter will explore the nature of suspicion and its various incarnations and variations in both interpersonal and technology-related contexts before the specific methodology used to address the overarching research question will be presented.

CHAPTER 2: LITERATURE REVIEW

Interpersonal Perspectives

To explore the nature of user suspicion toward IT, it is appropriate to first explore the nature of the foundational construct of interest: suspicion. As mentioned in the previous chapter, suspicion per se has traditionally and more explicitly been addressed within interpersonal contexts. Thus, the present discussion will also begin with an examination of suspicion grounded in the interpersonal literatures before turning to discussions of suspicion, and suspicion-related concepts, from more technology-centric or technology-specific perspectives.

Suspicion

Several definitions of suspicion have been proposed in the interpersonal literature. For example:

- Deutsch (1958) defines suspicion from the aspects of expectations (anticipation of behavior) and motivational relevance (positive or negative affect on a person's interests). A person becomes suspicious if his/her expectations are not met and the behavior results in a negative motivational consequence to that person.
- Kee and Knox (1970) defined suspicion in terms of a person's uncertainty of another person's trustworthiness.
- Fein, Hilton, and Miller (1990) define suspicion as "a dynamic state in which the individual actively entertains multiple, plausibly rival hypotheses about the motives or authenticity of a person's behavior" (p. 1165).

- Hubbell, Mitchell, and Gee (2001) define suspicion as a negative expectation of a perceiver based upon inferences made about an actor as a result of information that the perceiver has been given.

While each of these definitions may capture the essence of suspicion in a variety of contexts, there are common elements. First, the overarching element is the notion that suspicion is an active process or what Fein (1996) refers to as "the psychological state of suspicion." (p. 1164); a person makes a cognitive effort to ascertain the "reality" of a person's motives and behaviors. Second, suspicion is a negative expectation and an uncertainty regarding another's motives and attributed behavior, both of which are considered within the suspicion process. Finally, these definitions suggest that suspicion is a multifaceted process with a beginning, where suspicion is generated; middle, where a suspended judgment exists; and an end, where an actor's true motives and behavior are ascertained. To fully understand suspicion one must therefore examine the process of suspicion from beginning to end.

The "Process of Suspicion"

Generating Suspicion

The process of suspicion begins as a result of any of a number of factors. The generation of suspicion is marked by the point at which a person is aroused by a particular event or induced to become suspicious. This condition is a situation-dependent arousal or "state suspicion" (Levine and McCornack, 1991) defined as "a belief that communication within a specific setting and at a particular time may be deceptive" (Ibid., p. 328). For example, the Prisoner's Dilemma (PD) Game has been used in research to

study cooperative behavior (Deutsch, 1958). The PD game involves participants who each must make one of two choices: a cooperative choice, which offers the best outcome for each player, with little payoff for all players; or a competitive choice, which offers the greatest outcome to one player, but severe detrimental loss to the others. The issue was whether or not a player would exploit the other's generosity in the hopes that he will gain the most benefit, regardless of the consequences to the other player. Therefore, each player's decision to cooperate or compete was based on uncertainty of the other player's motivations. Hence, the rules of the game are such that each player is suspicious of other player's motives. Similarly, a salesman who is supposedly providing the "best deal" he can is more likely to be concerned with getting a higher commission on the sale than the welfare of the consumer. As a consumer, the "nature of the game" therefore naturally implies that the salesman's motivations are automatically suspect. Both scenarios are examples of situations in which suspicion is implicitly induced prior to an interaction.

Hubbell et al. (2001) found timing of aroused suspicion affects subsequent cognitive processing. Specifically, suspicion arousal prior to an interaction resulted in a higher initial suspicion, than those who were not aroused prior to an interaction. However, according to Stiff, Kim, and Ramesh (1992), it is unlikely for people to become suspicious on their own; instead, third-party information can arouse suspicion. This aroused suspicion could also be reduced or increased by further interaction with the actor, or another party. In general, such arousal prior to or at an initial interaction is often high enough to influence the decisions made within the suspicion process that ensues.

Suspicion could also be the result of a predisposition referred to as a generalized communicative suspicion (GCS). According to Levine and McCornack (1991), GCS is an

inherent belief that all incoming communication behaviors from others are deceptive. Although not all people are predisposed to make this generalization, this particular type of suspicion is not situationally-dependent as was state suspicion. Both state suspicion and GCS are precursory to any cognitive processing judgment about a particular message. However, people who are predisposed to GCS are more astute in the subsequent cognitive processing judgment, than individuals who are not predisposed to GCS. Therefore, the concepts of state suspicion and GCS should not be overlooked as relevant independent variables in suspicion-related research (Ibid.).

A person may also become suspicious when an expectation is not met. An expectation is a person's preconception that an actor will behave according to the inferences made by that person or as a result of information about that actor (Hubbell et al., 2001). McCornack and Parks (1986) found as a relationship develops partners tend to become less discerning of each other's behaviors and begin to generalize their expectations of each other. Hence, as relational development increases the level of uncertainty of each partner decreases (Ibid.). Deutsch (1958) viewed such expectations as anticipated behaviors that were indicative of a person's underlying motives or rationale for action. For example, if a person trusts another to carry out a relatively simple task, that person's expectation is that the task will be accomplished. However, if the task is not completed, the trusting person loses confidence in the other person and therefore becomes suspicious as to why the other person was unable to complete the task. The trusting person may begin to question and attribute this failure to not only a person's efficacy, but possibly to the other person's motivations.

Finally, suspicion may occur as a result of dispositional inferences made about another person even when an opposing explanation is provided (Fein et al., 1990). A person makes a dispositional inference when that person judges another based solely on the behavior of the other person, without regards to the situation or the environment that may have caused the behavior. In other words, an observer may note that another person looks or behaves in such a way that triggers suspicion, even though an explanation is provided that contradicts the inferred behavior. For example, a woman drops her books and a man stops to help her pick them up. An external observer may conclude a situation in which a person is helping another in a time of distress. However, if the woman was young and pretty, and the man and woman are not married (as assumed by the lack of a ring on his and her finger), then the external observer may suspect that the man had an ulterior motive. Perhaps the man's deed was not sincere, but an attempt to meet a pretty woman. What if the woman wasn't pretty? Would the man have behaved as he did?

People who typically make dispositional inferences based on their observations of others may be misled by ignoring the environment or situation – referred to as the fundamental attribution error (Ross, 1977) or correspondence bias (Gilbert and Jones, 1986). Although this may not be a valid way to determine another person's true motives, it does provide a relatively practical and initial justification as to what that person's behavior represents. Thus, to ensure the validity of one's dispositional inference of another person's behavior, an active cognitive process ensues that takes into account the situation (Fein, 1996) – an important part of the next step in the suspicion process – maintaining suspicion.

Maintaining Suspicion

As suggested thus far, initial suspicion may be attributed to several factors; however, once suspicion is initiated, there is an intricate and associated sub-process left to run its course. Whether suspicion is a result of situational arousal, GCS, unfulfilled expectation, or dispositional inference, the next stage of suspicion generally involves a person's attempts to confirm an actor's behavior or motives underlying the observed behavior. According to Fein (1996), a suspicious person uses a more active method of cognitive processing (as opposed to an unsuspicious person) used to ascertain a person's behavior or ulterior motives. This intense cognitive processing is what Fein (1996) refers to as a psychological state of suspicion or "suspended judgment." The bulk of the suspicion process is consumed by this suspended judgment and it may become an enduring step because a person may remain in a suspicious state due to the cognitive complexities involved in the attempts to determine an actor's true motives and behavior.

Perhaps the best representation used to model this process of suspended judgment (Fein, et al., 1990; Hilton, Fein, and Miller, 1993; Fein, 1996) is the person- (or social-) perception construct developed by Gilbert, Pelham, and Krull (1988). The construct consists of three sequential stages (Ibid, p. 374):

> (a) Categorization (i.e., identifying actions);
> (b) Characterization (i.e., drawing dispositional inferences about the actor);
> (c) Correction (i.e., adjusting those inferences with information about situational constraints).

The three-stage construct begins with categorization, which Gilbert et al. (1988) considers a simple and relatively routine process that devotes little cognitive effort. Categorization is essentially an observation made that is obvious, such as "We see Henry

playing poker rather than simply moving his fingers, Herbert cheating rather then simply taking a card from his sleeve" (Ibid., p. 734). According to Trope (1989, p. 302), "In everyday life, task demands and the perceiver's own goals frequently require the use of the immediate behavior to predict how the actor will act toward other objects in different occasions and circumstances."

Although categorization is discussed in this step of the suspicion process, identifying a behavior is typically done prior to a suspended judgment. Trope (1989) suggests the identification of a behavior or situation is prior to making a dispositional inference. Categorization may be a means to provide an immediate judgment at the onset of a social interaction; however, the evaluation does not necessarily stop there. According to Hilton, et al. (1993), categorization is an initial acceptance of an observed behavior, but then a person follows it up by making a dispositional inference about another person's behavior and taking into account conceived situational variables (i.e., characterization). Because categorization is a simple process of identifying a behavior, it is relatively quick and not cognitively demanding – as opposed to the subsequent processes of characterization and correction.

The next step in the three-stage process is characterization. Gilbert (1991) found that the components of believing in something perceived (i.e., an object, person, action, self), a person must first identify (categorization), and then make an evaluation of that perception (characterization). A distinction between higher (active processing) and lower (passive processing) orders of reasoning was posited by Gilbert et al. (1988), such that "One passively has a perception, whereas one actively draws an inference" (p. 743). It follows that suspicion is not simply a result of a person's perception of another, but it

also includes an inference of some kind. Fein (1996) posits that suspicion produces active perceivers who are reluctant to make quick characterizations about an inferred behavior. Thus, the author suggests characterization is not automatic in suspicious perceivers; instead, one must apply certain inferential rules to achieve a state of characterization.

One such inferential rule is the anchoring principle (Tversky and Kahneman, 1974; Quattrone, 1982). An initial assessment presents an "anchor" for making any adjustments to subsequent judgments; however, the anchor may also change as a result of an active perceiver's reevaluation of the characterization stage (Gilbert et al, 1988. For example, a perceiver notices a person using a modified coat hanger to break into a car (e.g., categorization) and makes an inferred judgment (e.g., characterization) that this is an attempt to steal the car or any belongings in it (e.g., the anchor). However, further observation yields the person does not look like a criminal (based on his knowledge, experience, and perception); therefore, he decides the person simply locked his keys in the car (e.g., adjustment to the anchor). On the contrary, the perceiver observes the person hurriedly get into the car and speed away. The perceiver again adjusts his judgment to reflect the original anchoring judgment as true.

The aforementioned characterization stage provides an assessment that could lead to a confirmation or disconfirmation of suspicion, or lead one to remain in a state of suspended judgment until more information is made available to substantiate an ultimate verdict (Hilton et al., 1993). The correction stage is where much of the cognitive resources are devoted as a person reevaluates multiple hypotheses, situational factors, and other information that supports correction or adjustment of the initial characterization (i.e., interpretation of the inferred behavior). This seemingly unremitting process, which

may vacillate between the stages of characterization and correction, requires a conscious and deliberate effort in order to come to an accurate response (Fein, 1996). For example, returning to the aforementioned scenario of the person breaking into a car, the perceiver decides to take into account the situation. The perceiver realizes the person may have been late for an appointment as a result of locking his keys in the car and spending a significant amount of time trying to break into it. Suspicious perceivers actively pursue competing options and additional information toward a salient confirmation of the dispositional inference, while taking into account situational factors, and therefore reduce the chances of a correspondence bias (Fein, 1996).

Concluding Suspicion

Finally, suspicion ends when a person no longer questions an actor's motives and behavior because a determination has already been made. Marchand and Vonk (2005, p. 251) state that "suspicion is a dynamic process that unfolds over time as people grapple with the possibility that an actor has ulterior motives, and then become convinced." The authors also suggest that the speed of the suspicion process may be affected by individual personalities. For example, people who have a high "need for closure may be quicker to jump through the process and conclude that an actor is insincere" (Ibid., p 254). The process involves a wealth of cognitive resources as a result of attempting to find the truth behind an actor's behavior as described in the previous sections. Once the perceiver arrives at a final judgment as a result of the suspicion process, suspicion ends because there are no longer multiple, rival hypotheses. Exactly what is the nature of this final judgment? As will be discussed in a section to follow; the process of suspicion ends when

a perceiver ultimately arrives at a decision to trust or distrust; hereafter referred to as a "trust-decision." It is important to note that further mention of a "trust-decision" in this study is synonymous with resolving the suspended judgment of the suspicion process.

Bias Effects on the Suspicion Process

The suspicion process is not free from certain biases that have a direct effect on the process itself. The truth- and lie- biases affect the cognitive processing of the characterization and correction stages within the three-stage suspicion process. Truth-bias is a person's inclination toward processing another person's message as true (McCornack and Parks, 1986). Stiff et al. (1992, p.328), suggested that the "truth bias represents a default mode that guides the processing of relevant information." According to Marchand and Vonk (2005), some people are inclined to accept everything they see at face value. In other words, when a person is provided information, whether it is from a third-party or other indications, that person will accept such information as true. The truth-bias exists as a result of well-developed relationships (Stiff et al., 1992). Findings have shown that as a relationship develops, partners tend to believe in each other's trustworthiness and rarely question it (McCornack and Parks, 1986); therefore acceptance of trustworthiness, as a result of the truth-bias will preclude the active characterization and correction stages of a suspended judgment.

Unlike the truth-bias, the lie-bias is "a cognitive-processing bias toward decoding all incoming messages as deceptive" (Levine and McCornack, 1991, p. 328). The difference between lie-bias and GCS (previously mentioned under generation of suspicion) is that GCS is based on beliefs that are inherent prior to making any judgment

(or arduous cognitive effort) based upon information provided, whereas the lie-bias involves the cognitive processing of information presented. Therefore, a person who is predisposed to the lie-bias does not remain in a suspended judgment for long, if at all (Ibid.). As a result of a biased processing suggesting all information as false, a person will consequently and quickly validate his/her suspicion, due to his/her negative perception of the target's motives. Therefore, a lie–bias, like the truth-bias, affects the process of suspicion by either expediting the suspended judgment or excluding the suspended judgment altogether.

Trust

No discussion of suspicion would be complete without a discussion of trust. Trust is a concept intimately related to its "darker cousin" – suspicion (McCornack and Levine, 1990, p. 219), because as proposed in the aforementioned suspicion discussion, a "trust-decision" is the end-state of the suspicion process. In fact, McCornack and Parks (1986) suggest even a slight state of suspicion is helpful in making a trust-decision. In addition, Marchand and Vonk (2005) propose "the process of suspicion may apply to any situation in which a person's behavior can be guided by multiple motives, thus causing perceivers to hold multiple hypotheses, or doubt whether their initial judgment was correct" (p. 254). The concept and process of suspicion is a psychological state resulting from situational, or outside influence, predispositions, expectations, certainty (or uncertainty), or behavioral (dispositional) inferences, all which can be affected by biases. As will be demonstrated in the following sections, so too is the notion of trust.

Trust is a vital part of a wide range of relationships, from romantic relationships to organizational relationships (Whitener, Brodt, Korsgaard, and Werner, 1998). We place trust in our government, military, businesses, doctors, babysitters, and so on. It is fundamental to social interactions in groups and at work in hopes that everyone will contribute and cooperate in order to meet established goals. We tend to trust because it is a necessary and desirable aspect in our diverse interactions with others, and that if we did not trust, then we would never know (Gambetta, 1988).

Trust is a complex concept with research that spans several disciplines – psychology, sociology, philosophy, economics, organizational science and education (Tschannen-Moran & Hoy, 2000). Due to the breadth of trust research amongst several disciplines, each offering its own definition, confusion exists as to a single definition and conceptualization of trust. For example:

- Deutsch (1958) defines trust in terms of expectations (anticipation of behavior) and motivational relevance (positive or negative affect on a person's interests). A person trusts another if his/her expectations are met and the behavior results in a positive motivational consequence to that person.
- Kee and Knox (1970) defined trust in terms of a person's certainty of another person's trustworthiness.
- Rotter (1971, p. 444) defined trust as "an expectancy held by an individual or a group that the word, promise, verbal, or written statement of another individual or group can be relied on."

- Lewicki and Stevenson (1998, p. 439) defined trust as "confident positive expectations regarding another's conduct."
- Rousseau, Sitkin, Burt, and Camerer (1998, p. 395) provided "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behavior of another."

The "Elements of Trust"

Clearly, trust, like suspicion, is a multidimensional construct. Each of the proposed definitions above provides contextual variations to the definition of trust; however, it is interesting to note the similarities and recurrence of various elements of suspicion within the proposed definitions of trust – elements such as situational and outside influence, expectations, certainty (or uncertainty), and dispositional inferences. Because of these similarities, it seems reasonable to conclude that the trust-decision is somehow tied to the suspicion process…but how? Rousseau et al. (1998) conducted an extensive multidisciplinary study of trust literature in order to come to a fundamental conclusion of the concept of trust. The authors posited that a trust-decision is a dynamic, rather than static process that changes over time (Ibid., p. 395). Thus, the suspicion process and the process of making a trust-decision are astoundingly similar.

Similarities Between the Elements of Trust and Suspicion

Similar to the suspicion process, the trust process is also based on expectations, certainty (or uncertainty), and dispositional inferences, all of which can be affected by biases. For example, like suspicion, the term *expectation* or *expectancy* is used often in defining trust. Deutsch (1958) suggests that expectations are anticipated behaviors and

Rotter (1971) defined trust as an expectancy that others rely on to do or behave in a dependable or trustworthy manner.

Both trust and suspicion include the element of expectations that support the cognitive process of making a trust-decision. In fact, initial factors of suspicion somewhat mirror initial trust-decisions, such that the confirmation or disconfirmation of trust (or suspicion) relies on an initial assessment, which provides an anchor for adjusting subsequent decisions (Tversky and Kahneman, 1974; Quattrone, 1982; Gilbert et al., 1988). In other words, the three-stage construct used in the suspicion process: categorization (i.e., identifying actions), characterization (i.e., drawing dispositional inferences), and correction (adjusting those inferences), is the same process used in a trust-decision.

According to Bottitta and Felici (2006, p. 1274), "people develop, over the course of their lives, generalized expectations about the trustworthiness of other people." A person may make initial trust-decisions based on their individual perceptions of reality, as a result of past experiences. This allows a person to generalize those experiences from one person to another (Rotter, 1967). For example, children who grow up in an environment where there is continuity and predictability in their care and other needs will likely develop a sense of trust toward others (Kephart, 2004). Thus, generalized expectations lead to predictability of another's actions, which also reduces uncertainty (e.g., the element of suspicion).

According to Lewicki, Tomlinson, and Gillespie (2006), trust is the positive expectation (as opposed to a negative expectation that leads to suspicion) a person expects from another despite uncertainty about another's motives and behavior; however,

as previously mentioned in this study, as relational development increases, the level of uncertainty decreases (McCornack & Parks, 1986). Thus, relationship development facilitates trust between partners as a result of a decrease in uncertainty of each other's motives and behavior. Therefore, the elements of certainty and uncertainty are interrelated because a person must have a level of certainty in order to trust. A level of certainty is essentially a degree of confidence one has in regards to the associated risk involved with one's expectations (Rousseau, et al., 1998). In other words, a decision to trust is a willingness to become vulnerable to another, which poses a risk due to the uncertainty of whether or not the other person will act appropriately (Rousseau, et al., 1998; Hudson, 2004). According to Hudson (2004), if one were completely certain, trust would not be necessary (such as if one was certain about another person's intentions).

The general use of dispositional inferences is also the same in the process of suspicion and making trust-decisions. Jones and George (1998) suggest that a person's trust involves a cognitive effort to give meaning to associated behaviors one observes through social interactions. In other words, a dispositional inference is made that provides a contextual definition of the social interaction, which then becomes a basis for a trust-decision. The role of dispositional inferences on making trust-decisions is quite common in social interactions. According to Gilbert & Jones (1986), "people conceptualize behavior as the product of an actor's personal dispositions" (p. 269). Although making dispositional inferences takes a certain level of cognitive processing, it is not, however, the sole determinant of making a trust-decision (Quattrone, 1982; Trope, 1989). As previously mentioned, dispositional inferences are part of the characterization stage of the suspicion process, so too is it part of the trust process; however, both processes also

involve a stage of correction. Together the characterization and correction processes are a bulk of the cognitive processes of suspicion and trust.

The aforementioned discussion, suggests that Gilbert et al.'s (1988) three-stage construct: categorization, characterization, and correction, is a cognitive process used by both the suspicion and trust processes. Like the suspicion process, the decision to trust requires a person to gain a certain amount of knowledge or information to make that choice. According to McKnight, Cummings, and Chervany (1998), cognitive processes allow individuals to gather information and make initial judgments in order to form impressions of another person's trustworthiness. The initial trusting situation provides a foundational anchor to test whether the trust-decision was valid and allows one to adjust accordingly (Tversky & Kahneman, 1974; Quattrone, 1982; Gilbert et al., 1988). Hence, the suspicion process, which involves a psychological or cognitive effort to determine a person's motives and behavior, is the same process involved in determining another person's trustworthiness.

Finally, trust may be situationally-dependent or influenced by a third-party. Lewis and Weigert (1985) stated, "We cognitively choose whom we will trust in which respects and under which circumstances" (p. 970). However, trust is not gullibility, although some people are prone to act in such a manner. Instead, a decision to trust reflects experience in particular situations (Rotter, 1980). For example, when a worker goes in for a job evaluation, he trusts his manager to give him a good rating based on positive feelings about the interaction and past evaluations that were rated high – a generalized expectation as a result of

experience (Bottitta and Felici, 2006). Trust via third-party influence is also dependent on experiences and expectations. One is willing to trust another based on whether the other person has shown consistent acts of benevolence toward the other (Whitener, Brodt, Korsgaard, and Werner, 1998).

Effects of Truth-Bias on Trust

As mentioned previously, the truth bias is a person's inclination toward processing another person's message as true (McCornack and Parks, 1986). The effect of the truth-bias on trust is the same as that on suspicion. Specifically, the fact that a person is inclined to trust another without collecting additional information and processing it objectively implies that the resulting trust-decision is biased and may not be correct. As suggested by Stiff et al. (1992), the truth-bias is a product of well-developed relationships. The authors suggest that increases in intimacy directly influence relational partners' ability to trust each other. Thus, the truth-bias skews a person's ability to make an accurate trust-decision (McCornack and Parks, 1986). Therefore, a person who is truth-biased will likely make a presumptive trust judgment, without further consideration of the possibility of another person's ulterior motives or behavior. In other words, the suspended judgment of the suspicion process (e.g., the process used to make a trust-decision) is bypassed.

Suspicion Prior to Trust

Discussion thus far has demonstrated significant overlap of the suspicion and trust-decision processes, enough so that one may be led to assume that the processes are concurrent or totally the same. However, this assumption is not entirely accurate because

a person does not make a decision to be suspicious; rather the decision is whether to "trust or distrust." Simply put, the final outcome of a suspended judgment is a trust-decision, not a "suspicious-decision." Thus, suspicion is ultimately the process that leads a person to a trust-decision.

According to Jones and George (1998), "At the beginning of a social encounter, each person does not simply assume that the other is trustworthy; rather, each suspends belief that the other's values may be different from their own – that the other may not be trustworthy" (p. 535). Clearly, it is this "suspended belief" that is synonymous to the "suspended judgment" of the suspicion process. Therefore, questioning another person's trustworthiness is, by definition, suspicion. It follows then that suspicion is an antecedent condition or process to arriving at or rendering a trust-decision. Fein (1996) suggests that a suspended judgment is necessary in order to avoid being "duped by another individual" (p. 1166). However, one can only be "duped" if another person betrays one's trust, such as through an unfulfilled expectation that results in a negative consequence to the trusting person. Therefore, in order to avoid what Rotter (1980) called "foolish trust" or "gullibility" (p. 1), and to make a good trust-decision, a person must first engage in the process of suspicion.

Deception

> Though fraud [deception] in other activities may be detestable, in the management of war it is laudable and glorious, and he who overcomes the enemy by fraud is as much to be praised as he who does so by force.
>
> - Nicollo Machiavelli, *Discourses*, 1517 (Source: JP 3-58, p. II-1)

Trust and suspicion are clearly quite closely related concepts despite their stated complexities. For instance, trust may influence how quickly we become suspicious of others' actions, and our suspicions may impact the degree to which we ultimately trust others regardless of any additional information collected. Both perceptions may be affected by various forms of bias that could result in inaccurate judgments. However, there are other reasons why those judgments might fail us. For example, the object of our judgments may be intentionally trying to manipulate, circumvent, or outright deceive our various mechanisms and processes of suspicion and trust. What happens when the mechanisms of suspicion and trust don't lead us to the correct conclusions? What conditions or reasons might lead us to draw such faulty conclusions? Additional insight regarding the answers to these questions may be found in the pages of deception-based literature and research.

Deception – The word itself conjures up thoughts of wicked acts, but deception can actually be a good thing – depending on whether you are an instigator or receiver of the deceptive action. Deception is defined as "a deliberative attempt to mislead others" (DePaulo, Lindsay, Malone, Muhlbruck, Charlton, and Cooper, 2003) and "the manipulation of appearances such that they convey a false reality" and "includes both dissimulation (hiding or withholding information) and simulation (putting out wrong or misleading information)" (Druckman and Bjork, 1991, p.172). From these definitions, it follows that deception is not the same as lying, although it may include lying as a way to mislead others. Elaad (2003, p. 349) suggested, "All human beings are engaged in deception and are motivated to unfold the lies of other people."

Interpersonal Deception Theory

One of the more influential and well-cited theories in modern deception-related thought and research is the Interpersonal Deception Theory (IDT) developed by Buller and Burgoon (1996). The IDT is a robust theory within the interpersonal literature that blends the notion of suspicion with the complexities of deception and deception detection. The IDT is grounded in the idea that both sender and receiver of interpersonal deceptive communication are active participants and a sender's suspicion or trust has a continuous influence on both the sender and receiver. According to Burgoon, Buller, Ebesu, White, and Rockwell (1996, p. 258):

> Receiver suspicion is linked to sender behavior; it is made manifest through receivers' communication behavior; it is noticeable to senders; and its presence or the perception of it affects senders' own communicative behavior. Suspicion is thus a highly relevant element in understanding deception in interactive contexts.

The roles of sender and receiver are similar to perceivers discussed in the aforementioned suspicion and trust literatures. According to Burgoon et al. (1996), both senders and receivers bring into a social interaction "goals, expectations, and sometimes knowledge" relevant to the situation (p. 244). Behavioral inferences are made during this interaction in which initial credibility judgments (e.g., evaluation of a person's trustworthiness) are ascertained. Like the suspicion process, this initial credibility judgment serves as an anchor for subsequent adjustments. Adjustments to sender and receiver behavior are made as more information is processed during the interaction (Tversky and Kahneman, 1974; Quattrone, 1982; Gilbert et al., 1988; Burgoon et al., 1996). For example, a receiver may adjust or reevaluate an initial credibility judgment, manifested in a decision to trust or remain suspicious of a sender, as a result of

informational cues provided by further social interaction with a sender. On the other hand, a sender may also make adjustments to his/her own behavior as a result of informational cues presented from a receiver during a social interaction in an attempt to deceive (Burgoon et al., 1996). It follows that the suspicion process is inherent to the IDT. As anchoring and adjusting are parts of the suspicion process, so too are they parts of the IDT process conducted by both parties in an interaction.

Social interactions involve both sender and receiver attempts to identify informational cues presented by the other. The goal of a receiver is to identify cues that promote a trust-decision. In the context of deceptive communication, a receiver is specifically looking for deceptive cues. A receiver may identify cues that may incite suspicion leading to a verdict that a deceptive act is occurring or has occurred. For example, Burgoon et al. (1996) states that "based on social norms and expectations, greater unpleasantness and uninvolvement (e.g., nonimmediacy, inexpressiveness, noncomposure, and poor conversation management) should provoke greater suspicion" (p. 245). Thus, such cues are likely to take the form of any deviations from normal pleasant conversation and the level of the other's involvement in the interaction.

Senders have the daunting task of creating convincing messages through different types of verbal and nonverbal cues and by manipulating information, while managing the communication process (George and Carlson, 1999). Because senders are engaged in simultaneous tasks of sending a deceptive message and monitoring for suspiciousness from the target individual (DePaulo, et al., 2003) it is likely that leakage will occur. Leakage refers to those indicators that signal to others deception is present (Buller & Burgoon, 1996). However, receivers are also engaged in the dual task of discerning

incoming messages while attempting to hide their own suspicion. Thus, leakage of cues may come from both sender and receiver in attempts to deceive each other.

Indicators of deception, whether they are verbal or nonverbal, are considered deception cues, as they do arouse suspicion. Zuckerman, DePaulo, and Rosenthal (1981) conducted an extensive study on observable verbal and nonverbal deception cues. They noted that nonverbal deception indicators included body movements, facial expressions, and eye movements, whereas verbal indicators included voice inflections, such as pitch, tone, and rate of speech. Receivers who are attuned to these cues have a good chance of becoming suspicious, and therefore act on that behavior (McCornack and Parks, 1986; Burgoon et al., 1996). However, according to Toris and DePaulo (1984), sender's have an advantage, because they are able to take a receiver's responses to determine level of success and adjust accordingly. Although receivers are aware of cues and may even have detection strategies, receivers have the disadvantage of not knowing when a deceptive act occurs.

Effect of Truth-Bias on Deception Detection

Just as the truth-bias can impact the process of suspicion or the perceptions of trust; so too, can the truth-bias affect our ability to detect deception from others. According to Millar and Millar (1997), studies have shown that accuracy of deception detection is rarely over 60% and typically results in levels of chance. Zuckerman, Kernis, Driver, and Koester (1984) suggest receivers affected by the truth-bias tend to accept a sender's message and anchor it by providing it an initial value from which adjustments are made; however, making an adjustment when the deception is real results in an

inaccurate trust judgment. The reason a person may accept this initial value may be a result of a simplified decision process or heuristic (Stiff et al., 1992) that suggests that most messages are truthful (McCornack and Parks, 1986). According to Stiff et al. (1992), people who exhibit a strong truth-bias are involved in a "significantly less cognitive involvement" (p. 340) in the process of discerning truth from deception, as opposed to people who do not exhibit a truth-bias. Therefore, it seems reasonable to conclude that a person predisposed to the truth-bias is less motivated, and thus, less likely to search for deceptive cues that lead to detection.

Effects of Suspicion on Deception Detection

Clearly, the truth-bias negatively affects deception detection; however, according to Stiff et al. (1992), suspicion helps to offset the use of this heuristic (p. 329). Thus, the process of suspicion also has an influence on deception detection, in this case, a positive influence. Stiff et al. (1992) found, regardless of relational development level, suspicion is an important part of making a credibility judgment because suspicion leads to fewer decisions to trust. Biros (1998) also posited suspicion arousal strongly impacts deception detection ability, such as when a person is warned (e.g., via a third-party) prior to an interaction. As mentioned previously, suspicion aroused prior to an interaction results in a higher initial suspicion level than for those who are not aroused prior to an interaction, thus leading to increased cognitive processing (Hubbell et al., 2001). Therefore, aroused suspicion also causes perceivers to become more involved in the detection process (Burgoon et al., 1996), essentially motivating a person to detect deception and thus become more vigilant overall.

Summary of Interpersonal Literature Review

Suspicion is clearly a complex and active psychological process in which a person makes a cognitive effort to ascertain a person's true motives and behavior in order to come to a trust-decision (Fein, 1996). Both the suspicion and trust processes are a result of situational, or outside influence, predispositions, expectations, certainty (or uncertainty), or behavioral (dispositional) inferences, all which can be affected by biases. Trust, like suspicion, involves cognitive processes that allow individuals to gather information in order to make a judgment about another person. In addition, it has been suggested within the pages of this analysis that suspicion is a state of indecision and that a trust-decision is ultimately a decision made as result of that suspicion. Hence, suspicion is the process that leads to trust, and trust itself is one potential result of the decision that follows the process of suspicion.

Because deception is part of everyday life, and it is certainly important to those of us in a military context, detection of deception is necessary in order to protect oneself from being deceived by others. The importance of making a correct trust-decision via suspicion (the process of resolving a suspended judgment) is important to the notion of deception detection because it sides on the line of caution. Suspicion helps to eliminate gullibility and the truth-bias, which can hinder social interactions and relational development. However, both sender and receiver of deceptive messages are capable of deceiving the other, as well as being deceived. Therefore, the mechanisms and processes of suspicion, as well as one's ability to manipulate those mechanisms and processes, are critical to the identification of informational cues that are indicators of deception and hence the decision to trust or distrust.

Technological Perspectives

Discussion thus far has established the perceptual processes and mechanisms at work in the interpersonal "version" of suspicion, and those of the very closely entwined notions of trust and deception. However, we're still left to wonder how technology affects suspicion and trust; especially when the object of that suspicion and trust is no longer another person, but the technology another person might be using to communicate with others or simply the technology upon which critical information and processes may be created, stored, transformed, executed, or manipulated. It is these questions that inform the remainder of the literature review.

> Although perceivers may be fooled by nonsocial objects, they are not likely to suspect that these objects intended to behave in a particular manner to convey fictitious or misleading information. Our curses to the contrary, most of us realize that our computers do not intentionally crash whenever they sense that we are under unusually great amounts of pressure.
>
> - Fein (1996, p. 1164)

Human-Computer Interaction

The Association for Computing Machinery Special Interest Group on Computer-Human Interaction (ACM SIGCHI), the world's largest professional association of HCI researchers, define HCI as "the design, evaluation, implementation, and study of interactive computing systems for human use" (http://sigchi.org). The origin of HCI was traditionally focused on "ease of use," but today research goes beyond making a computer user's tasks easier or "user-friendly" and into the social aspects of the user such as perceptions and expectations (Bradley, 1998; Binstock, 1999). Thus, HCI is much more than designing computers to make it easier for people to accomplish certain tasks.

HCI is just as much, or even more, concerned with the human user as it is with the computing system.

According to Rozanski and Haake (2003), HCI provides a distinct point of view to the IT field because HCI research is primarily focused on understanding the user rather than the technology, "who they are, what they do, how and why they do things, and the contexts in which they work" (p. 180). The authors suggest HCI is a multidisciplinary field that includes disciplines such as cognitive and behavioral psychology, and sociology, combining with computer science, engineering, and graphic design (p.181). According to Binstock (1999), "Disciplines such as psychology and cognitive science play key roles in interaction design" (p. 3A). In fact, human attention, perception, and decision-making are elements of cognitive psychology that are considered essential knowledge for interface designers and HCI researchers (Rozanski and Haake, 2003).

Increasing use of IT has forced HCI interface designers to make HCI experiences easier and more fluid as they come to understand the similarities and differences associated with human-to-human interactions (Shechtman and Horowitz, 2003). There is evidence to suggest that interpersonally oriented perceptions such as suspicion and trust might also be the same kinds of perceptions we hold of IT/computers. Therefore, the following discussion draws parallels to the elements of interpersonal suspicion and trust within the context of the HCI literature.

The Basis of User Suspicion Toward IT

The Human-Computer "Social" Interaction

Bonito, et al. (1999) posited that HCI is perceived by many individuals as having the same relational implications as interpersonal or human-to-human interactions. For example, "virtual agents can be designed to appear and act more or less human" (Ibid., p. 229). With so much attention focused on the human aspects of the HCI, there is reason to suggest that human interaction with computers may be grounded in the same sorts of interpersonal perceptions and processes that are called into play during human interaction with other humans—those that are inherently social in nature. In fact, the notion of a human-computer "social" interaction may form the basis for why computer users become suspicious of IT.

Nass, Steuer, and Tauber (1994) conducted a study consisting of five experiments using experienced computer users (i.e., computer-literate college students), hypothesizing that the interaction of humans toward computers is fundamentally social. The authors reported that the responses of the participants in their experiments were indeed natural responses to social situations. For example, some people demonstrated tendencies towards certain social norms such as politeness toward their computers. In addition, the authors found that gender stereotypes applied to HCI when participant responses aligned with established social norms, such as "Males who praise are more likable than females who praise" (Ibid., p. 76). Participants associated different computer voices (i.e., computers synthesizing male and female voices were utilized in the experiments) as distinct social actors.

Other studies also lend credence to the socially-oriented HCI argument (Nass, Moon, Fogg, Reeves, and Dryer, 1995; Neumann, 1989; Lee and Nass, 2003). For example, Lee and Nass (2003) tested aspects of social interactions such as similarity-attraction (e.g., a person is more attracted to another who has a matching personality than one who does not match), consistency-attraction (e.g., people tend to like others who show consistent behavior because of their predictability), and social presence (e.g., a person may perceive an intelligent being or inanimate object is able to interact) in their HCI experiments (Ibid., p. 290). The authors found significant evidence, via participants' social responses to the aspects of social interactions, that human-computer social interactions can be established in a HCI.

Maintaining a socio-personal human-computer relationship is an increasingly important interest in HCI research. Bickmore and Picard (2005) suggest in order for users to experience an enjoyable, productive, and trusting interaction with a computer, the psychological aspects of human-human interactions must be addressed and incorporated into the design of the HCI and interface. Therefore, one of the goals for HCI researchers is to design social interfaces that aid the initiation and maintenance of the human-computer social relationship because it has an impact on perceptions of the computer (Shechtman & Horowitz, 2003). Due to the preponderance of evidence that suggests we have socially-oriented perceptions of our computers, the issue of suspicion towards IT will further be explored using some of the same theoretical lenses and perspectives that appeared in the interpersonal literature cited in the earlier sections of this review

Situational and Third-Party Aroused Suspicion

User suspicion toward IT may be aroused by one's situation or environment, or via third-party information. Fogg and Tseng (1999) suggest the situation in which one interacts with IT affects a trust-decision. For example, a majority of users simply use technology because it makes doing certain tasks easier, faster, and more reliable through the course of their personal or professional lives; therefore, it is reasonable to conclude that most users are not as discerning about their technology as IT professionals might be. Through the nature of an IT specialist's profession (e.g., military, computer & network security, law enforcement, management information systems), suspicion is quite often a necessity (Conti, Ahamad, and Stasko, 2005; Hollebeek & Waltzman, 2004).

Negative information from third-parties also influences suspicion. However, both the third-party itself and the information provided from the third-party must be perceived by the user as credible. Credibility, as mentioned in the previous interpersonal literature, is an evaluation of a person's trustworthiness. However, Fogg and Tseng (1999) suggest in evaluating computer credibility "a person makes an assessment of both trustworthiness and expertise to arrive at an overall credibility assessment" (p. 80). For example, users often rely on the advice of other users' inputs (which they themselves are perceived by the user as credible) regarding new technologies or applications, while the same companies developing these technologies rely on users' inputs to make modifications and improvements to their products (Binstock, 1999). According to Fogg and Tseng (1999), credibility of these companies in the form of their perceived reputation may impact user perceptions of such companies IT products and services. As suggested in the interpersonal literature, suspicion arousal prior to an interaction, whether it is

situationally-aroused or via a third-party, provides the initial anchoring decision that influences further cognitive processing involved in the suspicion process that follows. Therefore, user suspicion towards IT seems to draw upon the same initiating mechanisms as those found in interpersonal suspicion, as is the need for an initial anchor point from which further decisions or deliberations are then made.

Suspicious Predisposition

A predisposition of suspicion toward technology is referred to in this discussion as a generalized technology suspicion or what this author simply refers to as "GTS." GTS is similar to the generalized communicative suspicion (GCS) mentioned in the previous interpersonal literature (Levine & McCornack, 1991) and is a relevant element of IT user suspicion. However, unlike GCS, which is a belief that all incoming communication behaviors are deceptive (Ibid.), a GTS is a perception that there is reason to be suspicious of all technology. Note that the object of suspicion is the technology, not the information residing on it or information via a technology mediated communication. Discussion on suspicion caused by information residing on technology or technology mediated communication is discussed in a later section.

I propose, however, that people differ in GTS – whereas some people are predisposed to it, others are not. Just as well, Levine and McCornack (1991) did not imply that everyone had a predisposition for GCS, only that not all people are predisposed to make this generalization. GTS is a result of general assumptions people make about others and objects as a result stereotypes and culture (Fogg &Tseng, 1999). For example, we generally believe that people are truthful (McCornack & Parks, 1986:

Stiff et al., 1992); however, we do not hold the same regard toward salesmen. Similarly, people generally presume computers are good and trustworthy tools that provide accurate and timely information; however, computers that run simulations, instruct users, or perhaps are complex decision aids such as air traffic control systems are typically held suspect (Neumann, 1989; Fogg & Tseng, 1999).

Further argument suggests GTS is a result of a lack of faith in technology. "Faith" is synonymous to trust, confidence, and belief. According to McKnight and Kacmar (2007), "Faith in technology is different from faith in people because technology has neither volition nor motives" (p. 425). Faith in technology then implies a predisposed trust, confidence, or belief in technology, which therefore eliminates or bypasses the search for underlying motives and behavior (i.e., suspended judgment). However, not all people trust technology, as suggested in the aforementioned discussion on situational and third-party aroused suspicion, and even more so if one is "technophobic"(i.e., fear of technology as manifested by one's anxiety about the interaction and negative attitude toward technology or the interaction itself; Korukonda, 2004; Thorpe & Brosnan, 2004). Hence, GTS is a plausible argument that a predisposition of suspicion toward IT exists, just as GCS is in the context of interpersonal interactions.

Experience and Expectations

Muir (1987) posited that general expectations resulting from the predictability of computer behavior, as a result of experience, is directly related to trust. He further noted observations prior to and during a HCI lead to behavioral evidence that may support or contradict initial judgments (positive or negative) of a trust-decision. Because predictable

and reliable behavior of a technology facilitates trust in that technology (Flechais, Riegelsberger, and Sasse, 2006), we expect our computers to always be available (i.e., not break down) and consistently do the jobs they were designed for. Fogg and Tseng (1999) suggest first-hand experience over a period to time leads to a person's level of belief or "experienced credibility" toward a HCI. Therefore, repeated interactions with technology results in generalized expectations that we use as the basis or anchor for the subsequent decision of computer trustworthiness. Again, the anchor adjusts between interactions and during an interaction as a means of constant reevaluation (Muir, 1987).

The previous interpersonal literature suggests deviation from expectations may lead to suspicion of another person. Likewise, when it comes to technology, deviation of expectations may lead to suspicion of the technology. Binstock (1999) proposed that both the interface design and functionality of the technology are necessary to ensure user expectations are met, and to facilitate the maximum user experience. In other words, when systems are designed to ensure the HCI flows naturally and with relative simplicity, only then will the user experience be fully realized.

The "user experience" implies that the HCI is free from negative aspects associated with an interaction, such as an aesthetically unpleasing interface design, slow response, and functionally inept computer or application (Binstock, 1999). For example, errors such as a computer crashing or locking up, especially if these errors are experienced repeatedly, may lead to questioning a computer's credibility (Fogg and Tseng, 1999). Therefore, suspicion of the technology may be initiated due to the lack of a satisfactory user experience.

However, HCI designers and technology manufacturers must be careful not to over compensate their expectations of the user experience. Bonito et al. (1999, p. 236) found the manipulation of human-like qualities of anthropomorphic interfaces used in their study did not affect participants' evaluations of HCIs as anticipated. The authors predicted the more human-like an interface was, the more a human participant in a HCI would evaluate the interaction as positive. Instead, the interface did not match user expectations because they viewed the interface as so unrealistic or unbelievable that it invoked user suspicion toward the interface (Ibid.). Hence, the study demonstrated that generalized user expectations can affect the expectations of HCI designers if designer expectations are impractical or do not match user expectations.

Dispositional Inference Judgment

As suggested in the aforementioned discussion, HCI research extends into the social, cognitive, and behavioral aspects of the user. One of the elements of suspicion (and trust) is the notion of dispositional inference, an inference which also applies to the study and practice of HCI. For example, computer users make inferences toward computers based on "aesthetics and perceived usability" (Murphy, Stanney, and Hancock, 2003). Specifically, the authors suggest that there is a correlation between the way a computer (or interface) looks and its perceived usability. In other words, computer design may invoke either positive or negative affect toward the functionality of the computer depending on whether the design is pleasing or not to the user. Murphy et al. (2003) posits an "explanation for this phenomenon is the halo effect, which proposes that the most obvious or salient characteristic (such as if a user finds a computer aesthetically

pleasing) is perceived first and tends to bias perceptions and inferences that come after" (p. 1). Although this is an initial belief, and possibly contrary to rationale, it may persist until more information is gathered (Gilbert, Tafordi, and Malone, 1993). Hence, the halo effect is similar to the anchoring principle of the suspicion process.

According to Rozanski and Haake (2003), usability is a term used to recognize that "a system not only works, but also does what it is intended to do" (p. 182). For example, a laptop used by the typical student may be fine for everyday schoolwork, but may not be appropriate for a soldier on the battlefield that needs a ruggedized, lightweight version with different applications, interface, and interaction design. Both laptops may work fine, but each is appropriate to a different user, environment, and purpose. Thus, a user may make an inference concerning a computer's ability to perform a task simply by making an inferred judgment based on what the computer looks like, it's applications, interface, or interaction design. Fogg and Tseng (1999) call this "surface credibility" or in other words, "people *do* judge a book by its cover" (p.83).

Uncertainty and Self-Efficacy

Thus far, discussions on the elements of user suspicion toward IT were presented either implicitly or explicitly with the object of suspicion being the technology itself. However, there is also another object worth mentioning that may influence user suspicion toward IT – the object of self. Our nature and the nature of our cognitive processes imply that such suspicion and trust of IT can in fact be tied up in our own feelings about self and our abilities. Hence, the elements of uncertainty and self-efficacy are brought forth as relative aspects of our discussion of suspicion toward IT.

The interpersonal literature suggests suspicion may be generated as a result of uncertainty (Kee and Knox, 1970). The element of uncertainty applies to HCI as well, because a person places himself in a position of relative uncertainty – uncertainty about the technology. To elaborate, a computer (or any other technology) user, by initiating an interaction with a computer, places him or herself in an environment in which he may lack complete knowledge and experience of that system or its application (de Vries, Midden, and Bouwhuis, 2003). De Vries, et al. (2003) suggests that people are uneasy about using computers and software because of "a lack of knowledge about the application that causes users to feel uncertain about the outcome of a task" (p. 720).

Gross and Rosson (2007) conducted a study on computer user's understanding of computer security. All participants in their study were experienced computer users in their line of work, but had no special training or job tasks related to computer security. The authors found that participants had only a general knowledge and limited experience of hacker (including phishing) attacks, as well as the tools (e.g., virus scanners, spyware, and firewalls) necessary to prevent attacks. Furthermore, user behavior suggested inappropriate action a suspected security problem arose. For example, less than half of the participants in Gross and Rosson's (2007) study did not report legitimate security incidents to their IT staff when they suspected a security issue; rather they dismissed it as a possible functional computer error. Hence, uncertainty and self-efficacy seem to go hand-in-hand in the context of interaction with technology.

Self-Efficacy is a concept derived from the Social Cognitive Theory (Bandura, 1986) and refers to "people's judgments of their capabilities to organize and execute courses of action required to attain designated types of performances" (Ibid., p. 391). A

person's belief in his/her abilities affects his/her perception and evaluation of self in performance of tasks, whether it is mental, physical, social, or psychological. According to Bandura, "Among the different aspects of self-knowledge, perhaps none is more influential in people's daily lives than conceptions of their personal efficacy" (p. 390). Indeed, Compeau, Higgins, and Huff (1999) found that self-efficacy had a direct effect on computer use.

But does belief in oneself influence one's suspicion and trust of a computer system? Dassonville, Jolly, and Desodt (1996) suggest that "Trust between man and machine is a particularly imprecise and uncertain variable" (p. 319). The authors propose that the complexities of trusting a computer system is exacerbated by the fact that a user is part of the whole "system" and this adds a dynamic element to the HCI process. In essence, belief in oneself or perceived knowledge of one's abilities, as a result of being part of the larger "system," should have an effect on the interaction between human and computer and ultimately the perceptions of said computer through the course of those interactions. Although the research may be unclear at present as to *exactly* how self-efficacy impacts suspicion and trust, the fact that self-efficacy impacts any perceptions of technology at all suggest that it may also impact certain specific perceptions of technology to include those associated with notions of suspicion or trust.

Technologically Mediated Communication

Clearly, the elements of situational and outside influence, predisposition, expectation, behavioral (dispositional) inference, uncertainty, and self-efficacy are potential contributors to users' suspicion toward IT. In addition, the idea of a human-

computer "social" interaction suggests that the interpersonal notions of suspicion and trust may also play critical roles in our perceptions of IT. However, this study has, until now, focused on technological devices, such as the computer, as instruments of task production, with little mention on use of technology as a channel for information. What happens when we consider suspicion of technology used as a medium for interaction with another when the object of that suspicion may be blurred between the medium that facilitates the interaction (i.e., a technology channel) and the target of the interaction itself (i.e., another person, organization, etc.)?

According to Baltes, Dickson, Sherman, Bauer, and LaGanke (2002), computers and other computing technologies, such as the Internet, have transformed the way we communicate and created new ways in which we work together. Some examples of these technologies include the telephone, fax, email, document sharing, instant text-messaging, teleconferencing, and video conferencing (Horn, 2001; Baltes et al., 2002). In addition, the Internet is filled with websites that contain virtually any subject matter and cater to virtually anyone. From medical to financial advice, online shopping and banking, to sports, music, and academics, the list goes on and on. Although the advantages of technology-mediated communication (TMC) are abundant, many individuals find it very difficult to establish a trust relationship with another, especially via a technological medium where face-to-face interaction is not possible (Riegelsberger, Sasse, and McCarthy, 2005).

In particular, the concerns that are inherent to interpersonal face-to-face communications are intensified as a result of using TMC. A major concern, perhaps one

that may even lead to suspicion of technology per se, is the notion that technology may actually persuade us to do things contrary to what we emotionally, cognitively, and behaviorally would otherwise do. Berichevsky and Neuenschwander (1999) propose that people, in attempts to persuade others, use technology as a means to "amplify" their messages (Ibid., p. 51). In addition, many of the interpersonal or human-to-human processes such as suspicion and trust also manifest themselves in HCIs (Shechtman and Horowitz, 2003) as mentioned in the aforementioned human-computer social interaction section. Fundamentally, a TMC interaction is social in nature, more so than an exclusively human-to-computer interaction, because another person is involved in the interaction. Therefore, unlike HCI, suspicion of IT may stem from a user's perception of a person on the other end of a TMC interaction, rather than solely the technology itself. Because HCI designers are becoming increasingly focused on designing more social systems, it follows that the interpersonal mechanisms associated with suspicion may also be used and intensified in a HCI.

TMC facilitates suspicion as a factor on both ends of the interaction because whether a person is a sender or receiver, there is a constant cognitive effort to discern deception from truthful messages—effort that is complicated by TMC due to the lack of feedback from verbal and nonverbal cues that are inherent in face-to-face interactions (Giordano, Stoner, Brouer, George, 2007). Due to the nature of certain types of media, cues used for deceptive communication detection may even become distorted or lost entirely (Horn, 2001). For example, text messaging does not provide visual and audio cues, therefore a lack of verbal and nonverbal information may arouse suspicion and perhaps prolong a suspended judgment due to the lack of information needed to

disambiguate a trust decision (Riegelsberger et al., 2005). Even video media, which do provide visual cues, often do not provide the quality of nonverbal deception cues intrinsic to face-to-face interactions in order to discern truth from deception (Ibid.). Hence, use of TMC, as opposed to traditional face-to-face communications, provides users better capabilities to circumvent or at least diminish our suspicion and trust process, or in other words…deceive us. Certainly, the large volumes of deception literature related to the use of TMC to deceive others is evidence of the nefarious use of technology (Horn, 2001; Biros, George, & Zmud, 2002; Carlson, George, Burgoon, Adkins, & White, 2004; George, Marett, Tilley, 2004; Qin, Burgoon, & Nunamaker, Jr, 2004).

In summary, the reason for which it might be difficult for some to disambiguate their feelings about suspicion towards IT with suspicion towards others using that IT to communicate with them is primarily due to the social interaction that takes place within a TMC. As mentioned, TMC is essentially a human-to-human interaction that uses technology as a medium to communicate; hence, there is a social aspect to TMC. However, the issues surrounding the "human-computer social interaction" discussed in the aforementioned sections also bring social factors into play for HCIs of the technologies themselves (Shechtman and Horowitz, 2003). It is logical to conclude that that many of the interpersonal elements of suspicion emerge in the context of an HCI, but may also contribute to user confusion as to who or what they are actually suspicious of…the technology, or the person they are interacting with via the technology.

Conclusion

The intersection of the concepts of suspicion, trust, and deception suggests a significant overlap between them. Much exists in the way of suspicion-, trust-, and deception-based literature that has an "IT flavor"; however, to date there have been few, if any, very pointed investigations that deal explicitly with the notion of what makes people suspicious of technology itself – not the information on that technology, nor the messages from others, or people with whom that technology interconnects us. What does this type of suspicion entail? Are the elements and mechanisms of suspicion of IT the same as those for interpersonal suspicion? What concepts from the interpersonal and HCI literature's treatment of suspicion, trust, and deception survive into the notion of suspicion towards IT? Are any of the elements of TMC-related suspicion and trust informative in such contexts? The following chapter will outline the specific methodology used to answer such questions before the results of the current study will be discussed, as well as the conclusions drawn from those results.

CHAPTER 3: METHODOLOGY

Overview

Because of the complexity surrounding the perceptions and processes associated with user suspicion towards IT, an exploratory and primarily qualitative approach was used to gather and analyze data relevant to the phenomenon of interest. In particular, a modified version of Northcutt and McCoy's (2004) Interactive Qualitative Analysis (IQA) was employed throughout this study. Significant portions of this chapter were based on the work of Turner (2006) and are used with the permission of the author. IQA is a qualitative systems-centric approach to data-collection and analysis that involves participant's perceptions, based on their experiences, of what they consider reality of the explored phenomenon. Hence, the outcome of the IQA method is to establish meaning of a phenomenon by using the "eyes" of participants who are closely related to the phenomenon, allowing those participants to identify the constituent elements of that phenomenon and propose and describe relationships between said elements. The following sections will outline the specific aspects of the IQA methodology used in this study, which include a focus group and report.

Focus Group

The purpose of an IQA focus group is to develop a sense of the various perceptual elements that are part of the problem/phenomenon under consideration. The focus group is a means of data collection that reduces researcher bias because the researcher simply acts as a facilitator for the IQA process while minimizing external influence toward the

participants and on the content of the data collected. Participants, known as *constituents* in an IQA focus group (Northcutt & McCoy, 2004), are free to identify and analyze their own elements that contribute to a problem/phenomenon. Through group discussion, constituents organize their own data into meaningful categories called *affinities*. Further analysis involves constituents "articulating their own perceived relationships of influence among the affinities" (Turner, 2006, p. 47). IQA is a system-centric approach and was an appropriate methodological approach for this research because the system in question is the social system existing between human and technology. According to Turner (2006) IQA "…seeks to capture the lived reality of individuals and their experiences, actively involving study participants in the mapping and depiction of their stories to fully explore a given phenomenon" (p. 47).

Focus Group Participants and Recruitment

The discussion up to this point has implied a generalized population of interest (e.g., IT/computer users). However, for the purpose of this study, a constituency of IT-professionals, who also happen to be Air Force graduate level students from the Air Force Institute of Technology (AFIT), was solicited to serve as study participants. The primary reason for the choice of IT professionals to serve as constituents was based on the assumption that people who have experienced, or are at least closest to the phenomenon being investigated, are best able to provide the details necessary to generate a robust understanding of the complex problem/phenomenon (Northcutt & McCoy, 2004). An IT professional as defined in this study is a U.S. Air Force communications

officer or civilian professional with at least 4 years of service and experience in their career field.

It was determined that 4 years in an IT-related field should provide for adequate knowledge and experience working with diverse technologies. This assumption was grounded in the fact that, in general, Air Force communications officers are placed in diverse technical type positions such as monitoring and maintaining base or Air Force wide network traffic, providing phones (analog or IP), radios, cell phones, computer hardware/software, in addition to security, policy development and management associated with these functions, to include project or program management. Furthermore, the constituents were all graduate students attending an Information Resources Management (IRM) degree program.

The AFIT IRM program prepares graduates for leadership roles encompassing the operational, strategic, and tactical use of IT by exploiting the latest technologies, creating successful policies and processes, and applying sound management techniques to gain superior military advantage over adversaries. Discussion and research of the latest issues surrounding IT in general, such as the use and adaptation of technology, as well as security and management of technology from personal and organizational contexts, is a relevant part of the IRM program. Hence, the focus group constituency of Air Force communications officers and civilian professionals reflected the sort of diversity in work and educational experience and perspectives on IT appropriate to explore suspicion of IT in its many possible forms and incarnations from a very theoretically compelling perspective.

Recruitment was conducted through email announcement and word of mouth by the principle researcher to all 31 AFIT IRM graduate students in the 2008 graduating class. A total of 15 male participants agreed to join the focus group for a response rate of 47%. As an incentive, participants were given the opportunity to place their name in a drawing to win monetary prizes that included a first-, second- and third-place winner, with first-place having a significantly larger amount. The drawing was held immediately after the focus group meeting.

Focus Group Preparation

The focus group session was conducted in a closed conference room in order to avoid distractions. All constituents were briefed on ethical issues regarding research participation and the importance of the study. Constituents were also set at ease to foster a relaxed atmosphere in order to facilitate the free flow of ideas needed for the subsequent step of brainstorming. Because all constituents knew each other and many of them had already worked together in groups as a result of attending the same graduate program, all were already comfortable working with each other. In addition, all were reminded by the principle researcher that nobody was evaluated on their inputs; rather, they were simply encouraged to take an active part in group discussion and that each of their inputs were important and relevant to the study. Each constituent was provided markers and note cards. The constituency was given a brief overview of the focus group process (i.e., brainstorming, grouping of ideas, and establishing influence relationships between the ideas). A brief *question and answer* session was conducted to ensure the

constituency understood the process. Once the principle researcher felt each member had a good idea of the focus group process, the exercise began.

Identifying Factors/Affinities

A mental exercise was first conducted in which the constituency was asked questions designed to invoke experiences, perceptions, impressions, emotions, and anything else that came to mind as it pertained to suspicion of technology. The group was told to visualize internally any and all of their thoughts and experiences relating to suspicion of IT, and then instructed to silently and individually brainstorm ideas, perceptions, emotions, and anything else of relevance and write those thoughts down – one thought per card.

After about 20-minutes, writing had come to a noticeable stop; each member was then asked to tape their cards to a wall in the conference room. The group was then asked to clarify the meaning of each card, including ambiguous cards, to ensure all members of the group understood the meaning of each card without any direct intervention on the part of the principle researcher. This was a self-guided exercise in which the cards' meanings were clarified and then grouped together to create meaning. All cards were addressed, at times with adamantly diverse opinions; however, group consensus of each card's meaning was eventually achieved after approximately 20-minutes.

After a 10-minute break, the constituency then worked together to categorize (i.e., made connections to) their individual experiences or components from the note cards into logical and meaningful groupings, sorting the cards into clusters which they perceived had similar meaning, a process referred to as *inductive coding* (Northcutt & McCoy,

2004). After constituents sorted the cards into their collective categories, a brief description of each category was provided via self-directed group consensus to ensure shared understanding and meaning of each "category" – similar to the preceding process used for individual cards. The categories were then identified, described, and given a distinct and relevant name by the constituency itself. At this point, the named category was referred to as an *affinity* (Ibid., 2004). An example of the aforementioned process of categorizing and affinities is illustrated in Figure 1.

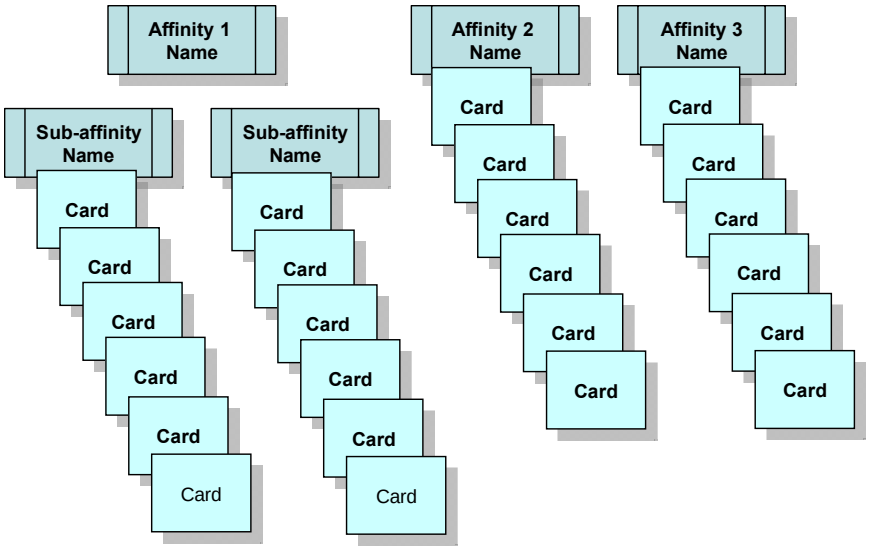

Figure 1. Focus Group Card Sorting and Affinities (Source: Turner, 2006)

Identifying Relationships Among Factors/Affinities

After affinity names were given and the constituency was content with their results, the constituents were given a 15-minute recess to allow time for the collection and printing of the voting sheets, also known as an *Affinity Relationship Table (ART)*. Table 1 is an example of an ART with six affinities. The ART gave constituents the opportunity to reflect on the nature of every possible relationship between every possible

pairing of affinities. Once the group reconvened, individuals were asked to use the ART to identify the nature of the influence relationships between all possible combinations of the affinity pairs (i.e., based on their individual perceptions), followed by a description of each relationship.

Table 1. Sample Affinity Relationship Table (Source: Turner, 2006)

Focus Group Affinity Relationship Table	
Affinity Name 1. Affinity 1 2. Affinity 2 3. Affinity 3 4. Affinity 4 5. Affinity 5 6. Affinity 6	**Possible Relationships** **A → B** **A ← B** **A <> B (No Relationship)**

Affinity Pair Relationship	Example of the relationship either in natural language or in the form of an IF/THEN statement of relationship
1 → 2	
1 3	
1 4	
1 5	
1 6	
2 3	
2 4	
2 5	
2 6	
3 4	
3 5	
3 6	
4 5	
4 6	
5 6	

The ART included a space for the participants to indicate the direction of influence between affinities such as: A influences B, B influences A, or no perceived relationship between affinities. If an individual thought two affinities influenced each

other equally, they were told to pick only one (e.g., the stronger) influence relationship. For example, a constituent who felt strongly that affinity 1 influenced affinity 2 would place a right arrow between the pair in the ART as illustrated in Table 1. The constituents continued this process until their ART form was completed.

The constituency was also asked to provide a brief description of each influence relationship in the form of *cause* and *effect* or *if/then*, an activity referred to as *theoretical coding* (Northcutt & McCoy, 2004). Constituents wrote descriptions on their ARTs in the space provided next to each affinity pair relationship. The principle researcher encouraged constituents to provide concrete examples relating to each constituent's perceptions or experiences because examples were considered ideal for describing their individual propositions of relational and directional influence of one affinity toward another. Although each individual was asked to do this, some chose not to provide a specific example; however, each constituent at least provided a completed ART with a full articulation of the affinity pair influence relationships for a total of fifteen ARTs. After the principle researcher collected each completed ART and the incentive drawings were conducted, all constituents were dismissed and the principle researcher collected all note cards while keeping them in their respective categories/affinities.

Report

The last phase of the IQA process was to generate a visual representation of the problem/phenomenon investigated. An illustration of the problem/phenomenon is provided via a systems influence diagram (SID) as depicted in Figure 2. The SID represents the common lived experiences and thought processes (or *mindmap*) of the

constituency as they pertain to the phenomenon under investigation. The diagram was drawn from the theoretical coding generated by the focus group constituents as recorded on the ARTs.

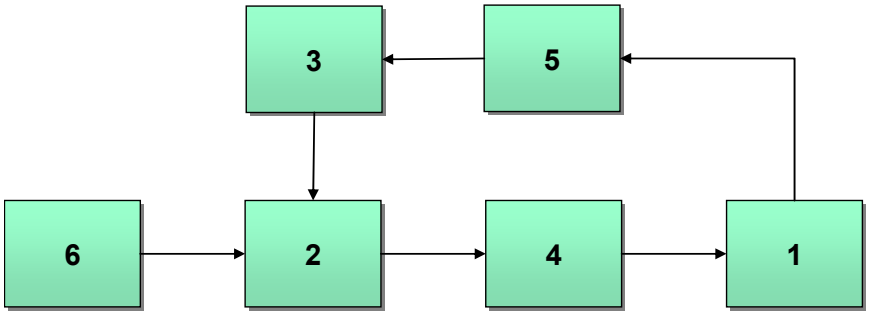

Figure 2. Sample SID (Source: Turner, 2006)

Hence, the problem/phenomenon was represented as a system of interconnected affinities showing cause and effect relationships as envisioned by the overall consensus of the focus group constituency. According to Turner (2006) "once a system of affinities and relationships is formulated and described, it essentially becomes a 'theory of lived experience' and can be 'exercised' and tested much as any other theory might be" (p. 247). Indeed, the process used to create a final SID required an extensive analysis of the data collected, including the perceived relationships of the individual constituents. In this instance, data collected from the focus group was compiled and analyzed to form the final SID and report. The following chapters will present a comprehensive summary and interpretation of these data and the detailed steps used to generate the SID and final report.

CHAPTER 4: RESULTS AND ANALYSIS

Focus Group Results and Analysis

The self-guided focus group approach provided a method to collect data with minimal researcher influence except as raconteur to facilitate constituent discussion and participation toward the problem/phenomenon as it relates to individual experiences or perceptions. Focus group constituents produced 85 cards and 8 affinities for analysis and interpretation.

Table 2. Focus Group Results

Affinities (elements) Relevant to User Suspicion Toward IT		General Meaning and Theme
1	**Corporate Trust**	Business needs conflict with consumer interests: IT companies, including manufacturers may restrict/delay the disclosure and distribution of the latest technologies, or prematurely distribute insufficiently tested products, both of which may lead one to distrust IT companies/manufacturers and their products.
2	**Data Loss**	Loss of data invokes suspicion: Data loss is attributed to obsolete IT products (e.g., hardware/software), or new systems (e.g., database or network).
3	**Ease of Use**	IT may be too complex: Users reluctant to use IT that is too difficult to use, or have too many functions.
4	**Policy**	User needs conflict with organizational policies: Management decisions to implement certain policies may lead to extreme constraint or overreaction to adapt or use IT.
5	**Privacy**	Information is susceptible to unauthorized disclosure: Users suspicious of IT as a media for social and professional interaction, because of nefarious entities monitoring or stealing information via an IT medium.
6	**Reliability**	User expectations of IT: Users expect IT to be predictable, or in other words do what it was intended to do without failure.
7	**Safety**	Fear of physical harm: Users expect IT to be safe, but are uncertain that companies are necessarily taking every precaution to ensure user's safety, as evidenced what is reported by news media or other sources.
8	**Security**	Security of the technology or system: Security means systems are patched, including necessary spyware and antivirus software, and physical security is in place as needed.

An overview of the results from the focus group's axial coding and affinity-naming activities are depicted in the *Focus Group Results* (Table 2), to include the group's general meaning and themes embodied by the contents of each note card under each of the eight affinities. A comprehensive explanation of the affinities will follow.

Affinity Reconciliation

Perhaps due to imposed time constraints, the focus group constituents seemed to express the need to make quick decisions in their *axial coding* activities. Furthermore, observations of the focus group's dynamics suggested several constituents' sense of urgency may have precipitated consensus of affinity names prematurely. A post-hoc analysis of each note card within each affinity was therefore accomplished unencumbered by the time constraints of the focus group meeting itself. Hence, the naming of the obtained affinities was re-examined and reconciled via triangulation process based on careful scrutiny of the contents of each note card, the affinity/category names provided by the focus group, reflections on the nature of focus group discussions, and the researcher's own knowledge of the relevant literature. Results of the affinity reconciliation process are presented in the following sequence of tables.

Credibility

The constituency felt IT companies and manufacturers are motivated to increase profits; however, they believe these companies do so at the expense of the consumer/user. In addition, some software includes backdoors as a means of tracking usage of such applications. When it comes to the latest technology, the high initial costs and misleading information lead to suspicion or distrust toward such companies, their products, and services. These credibility judgments regarding the motives of the companies behind various forms of IT (as well as the IT itself) may have been developed through personal experiences, but were often derived from external sources such as other users or from information provided by news sources (i.e., TV, radio, websites, blogs, etc.).

Table 3. Credibility Affinity

Focus Group Affinity: Corporate Trust	Renamed Affinity: Credibility
Business needs conflict with consumer interests: IT companies, including manufacturers may restrict/delay the disclosure and distribution of the latest technologies, or prematurely distribute insufficiently tested products, both of which may lead one to distrust IT companies/manufacturers and their products.	Although the group decided on naming this affinity "corporate trust", the general premise of inputs indicated questioning a company's trustworthiness (i.e., credibility), to include its products/services. The credibility of IT companies and manufacturers is an important and essential aspect of whether a user trusted a company, its products and services.

Personal Impact/Outcome

Based on personal experiences, several constituents admitted the loss of data had a detrimental affect on their perceptions of the technology – one that lead to user suspicion. Users blame obsolete technology, such as floppy disks, for losing data. They also blame new technology or systems that may not be implemented properly due to the

fact that they are so new that unforeseen negative events may happen; hence, leading one to suspect the technology to the extent of avoiding its use. Although the focus group titled this affinity "data loss," it was only when a user experienced the lost of *his* data that any impact was truly felt. Therefore, a decision was made to forego the specific term 'data loss' for the more general notion of 'personal impact/outcome.'

Table 4. Personal Impact/Outcome Affinity

Focus Group Affinity: Data Loss	Renamed Affinity: Personal Impact/Outcome
Loss of data invokes suspicion: Data loss is attributed to obsolete IT products (e.g., hardware/software), or new systems (e.g., database or network).	Several constituents had experienced loss of data either at work or at home. These negative experiences had an impact on their own perceptions of the technology, whereby they blamed the technology for the data loss.

Complexity

IT users seem to have a general expectation that IT products are complex. Users noted a general trend that technology is becoming increasingly more difficult to use and understand. Interestingly, group discussion made reference to the excessively 'thick' user manuals that accompany new products as an indication of the complexity of current IT products. Several constituents identified IT capabilities as more complicated with more functions than needed or used. One individual noted, "A new computer program is 'better' but the learning curve is too steep to successfully implement it." Constituents felt the relative uncertainty of such IT products invokes user suspicion due to the lack of a user's in-depth comprehension of the technology. Finally, technological complexity not only affects whether or not a person will use a particular technology, but may also

attribute to the difficulty of convincing others to use it, such as if one was a manager expecting his/her coworkers to use a new database application.

Table 5. Complexity Affinity

Focus Group Affinity: Ease of Use	Renamed Affinity: Complexity
The 'lack of' simplicity in a technological product may contribute to a user's reluctance to use it and negative perception of such technology.	The content of the cards and nature of the conversations seemed to center on larger issues of IT complexity rather than just the ease of use of the interface for that IT.

Organizational Context

The context of an organization is simply the situation or environment within which organizational members function. Inherent to any organization are the policies from which members must interpret and abide. However, interpretation and actual use of such policies may not always reflect the true nature of those policies as indicated by constituents who said that "policy does not always reflect user needs." The focus group constituents were all IT professionals in the Air Force; hence, the environment in which they use IT is bound and constrained by rather stringent IT policies which are indicative of the nature in which all directive policies tend to be developed and enforced. Constituents suggested that sometimes policies imposed by an organization, in this case the Air Force; generate negative user attitudes such as those that address the implementation or use of IT. An example given was the implementation of a new system a constituent felt was redundant of an existing system, yet the system was to be used as required by policy. Hence, IT policy, as part of the context of the constituent's organization, was an important issue that influenced user suspicions of that IT.

Table 6. Organizational Context Affinity

Focus Group Affinity: Policy	Renamed Affinity: Organizational Context
User needs conflict with organizational policies: Management decisions to implement certain policies may lead to extreme constraint or overreaction to adapt or use IT.	The group seemed to be focused on the term "Policy" as an appropriate name for this affinity; however, individual inputs suggest more than just policy – instead, it is the much larger "Organizational Context" in which they use IT.

Security of the Channel

Constituents felt that personal privacy was an important issue that made them suspicious of IT in general. The group suggested protection of privacy was a critical element needed in all technology products and services. Constituent inputs suggested a general distrust of IT communication media. For example, interactive voice, video and text communications in the form of cell phones, web cams, and email, respectively, were listed as IT communication channels a user suspected as having the potential to jeopardize one's privacy. Group consensus noted the lack of security in IT communications "leads to fear of using email, chat, and even online forums or blogs." The constituency's knowledge of security vulnerabilities that exist in various communication media suggested a general suspicion of IT-based communication channels.

Table 7. Security of the Channel Affinity

Focus Group Affinity: Privacy	Renamed Affinity: Security of the Channel
Information is susceptible to unauthorized disclosure: Users suspicious of IT as a media for social and professional interaction, because of nefarious entities monitoring or stealing information via an IT medium.	Most of the individual inputs suggested that the technological medium used or the "channel" was a security vulnerability that could put one's privacy at risk.

Expectations

The general theme expressed by the constituency was the notion that IT should have a degree of reliability and predictability. However, comprehensive interpretation of the individual inputs on the note cards implied that reliability and predictability were based on individual expectations of the technology. In addition, constituents noted their knowledge and experiences contributed to their expectations. For example, constituent inputs such as "bad experience with bugs in the operating system," and "excessive downtime created more stress" indicated a negative valence toward unmet expectations of the technology and not simply concerns about reliability per se. Hence, the majority of inputs suggested an emotional connotation toward unmet expectations resulting in negative experiences and contributing to a user's suspicion of the technology.

Table 8. Expectations Affinity

Focus Group Affinity: Reliability	Renamed Affinity: Expectations
User expectations of IT: Users expect IT to be predictable, to do what it was intended to do without failure.	Although the group decided to name this affinity "Reliability" the crux of the inputs suggested user "Expectations" of IT.

Vicarious Experience/3rd-Party Influence

Because no constituent admitted to experiencing an unsafe event regarding the use of a technology, the notion of "physical harm" that was originally expressed during the focus group as "safety" seemed suspect in its own right. However, the principle researcher's notes regarding focus group discussions indicated this idea of safety was not unsubstantiated; rather the constituents were basing their perceptions about IT safety on

what they had heard from others. Essentially, constituents were basing their ideas and perceptions on vicarious experiences instead of their own lived experiences.

Table 9. Vicarious Experience/3rd-Party Impact Affinity

Focus Group Affinity: Safety	Renamed Affinity: Vicarious Experience/ 3rd- Party Impact
Fear of physical harm: Users expect IT to be safe, but are uncertain that companies are necessarily taking every precaution to ensure user's safety as evidenced by what is reported by news media or other sources.	None of the constituents actually experienced an unsafe event (at least one that led to physical harm). Instead, individuals have a general suspicion of the technology based on vicarious experiences of others they read/heard about. The impact of third-party information was enough that constituents decided to include it as an element of suspicion.

Security of the Technology

The individual inputs indicated a general concern regarding the security issues that exist within technological hardware and systems. Inputs such as "portable hardware ignores security" and "unpatched or hacked systems" indicated a level of IT security consciousness from the constituents. It was not surprising that IT professionals in a security conscious context (such as the Air Force) would focus in on security.

Table 10. Security of the Technology Affinity

Focus Group Affinity: Security	Renamed Affinity: Security of the Technology
Security of the technology or system: Security means systems are patched, including necessary spyware and antivirus software, and physical security is in place as needed.	Most of the individual inputs suggested a general concern of the technological hardware and system.

Pareto Protocol and the Systems Influence Diagram

The IQA Pareto Protocol with Min/Max criterion was used to quantify the *theoretical coded* data as a means to create a visual representation of the system of perception and experience surrounding the affinities associated with IT user suspicion. The first step in applying the Pareto Protocol was to record the total number of votes for each affinity-pair relationship. Votes were counted from the individual ARTs and recorded on the *Theoretical Code Frequency Table* (Table 11). When a constituent provided a word-based example, the direction of influence indicated by the example was used; otherwise, the vote was tallied based on the direction of the arrow alone. As illustrated in Table 11, the 8-affinity system generated a total of 275 votes (not all affinity-pairs received a vote) with a total of 56 possible pair wise relationships.

Table 11. Theoretical Code Frequency Table

Theoretical Code Frequency Table			
Affinity Name 1. Credibility 2. Personal Impact/Outcome 3. Complexity 4. Organizational Context 5. Security of the Channel 6. Expectations 7. Vicarious Experience/3rd-Party Impact 8. Security of the Technology			
Affinity Pair Relationship	**Frequency**	**Affinity Pair Relationship**	**Frequency**
1 → 2	2	3 → 5	1
1 ← 2	9	3 ← 5	6
1 → 3	2	3 → 6	7
1 ← 3	9	3 ← 6	5
1 → 4	5	3 → 7	5
1 ← 4	5	3 ← 7	2

1 → 5	8	3 → 8	4
1 ← 5	6	3 ← 8	6
1 → 6	3	4 → 5	9
1 ← 6	10	4 ← 5	2
1 → 7	3	4 → 6	7
1 ← 7	5	4 ← 6	1
1 → 8	4	4 → 7	9
1 ← 8	10	4 ← 7	2
2 → 3	3	4 → 8	9
2 ← 3	4	4 ← 8	3
2 → 4	5	5 → 6	0
2 ← 4	7	5 ← 6	3
2 → 5	10	5 → 7	2
2 ← 5	2	5 ← 7	0
2 → 6	11	5 → 8	7
2 ← 6	3	5 ← 8	8
2 → 7	5	6 → 7	8
2 ← 7	0	6 ← 7	0
2 → 8	8	6 → 8	5
2 ← 8	5	6 ← 8	4
3 → 4	1	7 → 8	1
3 ← 4	12	7 ← 8	2
		Total	**275**

Pareto Principle

The total votes cast by the focus group participants were then sorted as illustrated in Table 12, the *Pareto Cumulative Frequency and Power Analysis Table*. The IQA method uses the Pareto principle to take into consideration the nature of people's individual and perceptual differences regarding the relationships between individual affinities by providing an unbiased protocol to calculate and represent a constituency's consensus of the overall hypothesized relationships between all affinities. As Turner (2006) explained:

Put in systems terms, the Pareto Principle states that in general, *20% of the variables in a system will account for 80% of the total variation in outcomes* (such as productivity or profit). The essential utility of the Pareto Principle is this: a minority of the relationships in any system will account for a majority of the variation within the system. Depending upon the variation of theoretical coding used, it is quite likely that there will be some disagreement among either individuals or subgroups about the nature of a given relationship. IQA uses the Pareto rule of thumb operationally to achieve consensus and analytically to create a statistical group composite. The *Pareto Cumulative Frequency Chart* provides an efficient method for achieving consensus. (p. 241)

Table 12. Pareto Cumulative Frequency and Power Analysis Table

	Affinity Pair Relationship	Frequency Sorted (Descending)	Cumulative Frequency	Cumulative Percent (Relation)	Cumulative Percent (Frequency)	Power
1.	3 ← 4	12	12	1.8	4.4	2.6
2.	2 → 6	11	23	3.6	8.4	4.8
3.	1 ← 6	10	33	5.4	12.0	6.6
4.	1 ← 8	10	43	7.1	15.6	8.5
5.	2 → 5	10	53	8.9	19.3	10.3
6.	4 → 5	9	62	10.7	22.5	11.8
7.	4 → 7	9	71	12.5	25.8	13.3
8.	4 → 8	9	80	14.3	29.1	14.8
9.	1 ← 3	9	89	16.1	32.4	16.3
10.	1 ← 2	9	98	17.9	35.6	17.8
11.	1 → 5	8	106	19.6	38.5	18.9
12.	5 ← 8	8	114	21.4	41.5	20.0
13.	6 → 7	8	122	23.2	44.4	21.1
14.	2 → 8	8	130	25.0	47.3	22.3
15.	2 ← 4	7	137	26.8	49.8	23.0
16.	3 → 6	7	144	28.6	52.4	23.8
17.	4 → 6	7	151	30.4	54.9	24.6
18.	5 → 8	7	158	32.1	57.5	25.3
19.	3 ← 5	6	164	33.9	59.6	25.7
20.	3 ← 8	6	170	35.7	61.8	26.1
21.	1 ← 5	6	176	37.5	64.0	26.5
22.	2 ← 8	5	181	39.3	65.8	26.5
23.	1 → 4	5	186	41.1	67.6	26.6
24.	1 ← 4	5	191	42.9	69.5	26.6
25.	1 ← 7	5	196	44.6	71.3	26.6
26.	2 → 4	5	201	46.4	73.1	26.7

27.	2 → 7	5	206	48.2	74.9	26.7
28.	3 ← 6	5	211	50.0	76.7	26.7
29.	3 → 7	5	216	51.8	78.5	26.8
30.	**6 → 8**	**5**	**221**	**53.6**	**80.4**	**26.8**
31.	1 → 8	4	225	55.4	81.8	26.5
32.	2 ← 3	4	229	57.1	83.3	26.1
33.	3 → 8	4	233	58.9	84.7	25.8
34.	6 ← 8	4	237	60.7	86.2	25.5
35.	2 ← 6	3	240	62.5	87.3	24.8
36.	1 → 6	3	243	64.3	88.4	24.1
37.	1 → 7	3	246	66.1	89.5	23.4
38.	2 → 3	3	249	67.9	90.5	22.7
39.	4 ← 8	3	252	69.6	91.6	22.0
40.	5 ← 6	3	255	71.4	92.7	21.3
41.	1 → 2	2	257	73.2	93.5	20.2
42.	1 → 3	2	259	75.0	94.2	19.2
43.	2 ← 5	2	261	76.8	94.9	18.1
44.	3 ← 7	2	263	78.6	95.6	17.1
45.	4 ← 5	2	265	80.4	96.4	16.0
46.	4 ← 7	2	267	82.1	97.1	14.9
47.	5 → 7	2	269	83.9	97.8	13.9
48.	7 ← 8	2	271	85.7	98.5	12.8
49.	3 → 4	1	272	87.5	98.9	11.4
50.	3 → 5	1	273	89.3	99.3	10.0
51.	4 ← 6	1	274	91.1	99.6	8.6
52.	7 → 8	1	275	92.9	100.0	7.1
53.	2 ← 7	0	275	94.6	100.0	5.4
54.	5 → 6	0	275	96.4	100.0	3.6
55.	5 ← 7	0	275	98.2	100.0	1.8
56.	6 ← 7	0	275	100.0	100.0	0.0
	Total Frequency	**275**	Equal Total Frequency	Equals 100%	Equals 100%	Power = CPF - CPR

Table 12 shows the same frequencies of theoretical coding as the previous theoretical code frequency table, except that they appear now in descending order of frequency. The four additional columns are:

1) ***Cumulative Frequency*** – Each successive entry provides the cumulative frequency of the number of votes cast for an affinity pair added to the previous total for a total number of 275 votes.

2) ***Cumulative Percent (Relation)*** – A cumulative percent calculated from the total number of 56 possible affinity pair relationships; hence, each relationship represents 1/56 or approximately 1.8% of the total possible number of relationships.
3) ***Cumulative Percent (Frequency)*** – A cumulative percent calculated from the total number of votes cast for each affinity pair relationship (275). Each successive entry provides the percent of votes cast for an affinity pair added to the previous total for a total of 100% affinity pair relationships.
4) ***Power*** – A factor used to identify and evaluate the optimal number of relationships to be retained in the representation of a perceptual system. Power is calculated as the difference between Cumulative Percent (Frequency) and Cumulative Percent (Relation).

Establishing a Cutoff

Essentially, the *Pareto Principle* is a statistical protocol used to provide quantitative decision-making criteria indicating relative weights or importance (i.e., power) of the qualitative data provided by the focus group. Hence, researcher bias was minimized as a result of using this protocol to establish the necessary statistical cutoff (based on the results of the Min/Max criterion of the Pareto Protocol). As illustrated in Table 12, row 30 is highlighted to indicate the cutoff from which all affinity-pair relationships located above and including the cutoff point was utilized to create the resultant System Influence Diagram, or SID.

The IQA method uses the Min/Max criterion of the Pareto Protocol, essentially the aforementioned 80/20 rule of the Pareto Principle, in order to establish a cutoff. According to Turner (2006), "In general, IQA systems modeling requires that the selected affinity-pair relationships account for at least 80 percent of the total variance, often at or slightly after the point where marginal gains in power begin to decline" (p. 68). Therefore, when the maximum variance (cumulative percent by frequency) reached 80

percent and no more marginal gains in power were realized by adding another affinity-pair relationship into the set of relationships that would be modeled in the final SID, that relationship marked the cutoff.

As indicated in Table 12, row 30, the maximum variance obtained at the cutoff was 80.4 percent and power was 26.8. If the frequency number (frequency sorted descending) of the affinity pairs repeats into rows beyond 80 cumulative percent of the ART votes, the cutoff is adjusted to reflect all occurrences of that frequency number prior to the change of next lower frequency (i.e. all affinity-pairings with a frequency of '5' are included even if some of the pairing appear at a point beyond which gains in marginal power no longer increase). In this case, the selected relationships with a frequency of '5' and higher accounted for 53.6 percent of the total relationships appearing in the ART voting forms, and 80.4 percent of the total votes recorded.

Conflicts

Conflicts occur as a result of the individual differences between the *theoretical coding* of affinity-pair relationships and occur when both A → B and A ← B relationships survive the Min/Max criterion of the Pareto Protocol. Because these types of relationships were above the established cutoff, either conflicting affinity-pair relationship was conceivably a "valid" explanation for indicating or explaining the direction of influence between two affinities. For the initial creation of a system influence diagram, only one of the two conflicting relationships is used as indicated in the *Conflict Relationship Table* (Table 13). The process to resolve conflicts is discussed in the next section.

Table 13. Conflict Resolution Table

Conflict Resolution Table					
Affinity Pair Relationship	**Frequency**	**Conflict?**	**Affinity Pair Relationship**	**Frequency**	**Conflict?**
1 ← 2	9		2 → 8	8	Use
1 ← 3	9		3 ← 4	12	
1 ← 4	5	Use*	3 ← 5	6	
1 ← 5	6	?	3 ← 6	5	?
1 ← 6	10		3 ← 8	6	
1 ← 7	5		3 → 6	7	Use
1 ← 8	10		3 → 7	5	
1 → 4	5	?*	4 → 5	9	
1 → 5	8	Use	4 → 6	7	
2 ← 4	7	Use	4 → 7	9	
2 ← 8	5	?	4 → 8	9	
2 → 4	5	?	5 ← 8	8	Use
2 → 5	10		5 → 8	7	?
2 → 6	11		6 → 7	8	
2 → 7	5		**6 → 8**	**5**	

Constructing the Interrelationship Diagram

Conflicting relationships used in the generation of a System Influence Diagram were resolved by initially choosing the relationship with the highest frequency while the relationship with the smaller frequency was placed on "hold" until it could be reconciled later. As illustrated in Table 13, the word "Use" indicates the conflicting relationship pair chosen as part of the initial SID; a "?" was used as a placeholder until after the initial SID was created. Note that the 1 ← 4 and 1 → 4 relationships had equal frequencies as indicated by the asterisks. The affinity-pair relationship 1← 4 was selected for inclusion in the initial SID because the frequency of influence *from* affinity #4 toward the other affinities was much greater than the frequency of influence *towards* affinity #4 from the other affinities. Furthermore, the majority of affinity-pair relationship frequencies

indicated common influence toward affinity #1. Hence, the 1← 4 relationship was the more "popularly perceived" of the two relationships in terms of the "flow and direction of influence" and was therefore used until the conflict was resolved.

The Interrelationship Diagram (IRD) was then used to provide a tabular summary of the obtained affinity-pair relationships from the previous Pareto Protocol and determine the relative position of each affinity within the system. By utilizing the information provided by the *Conflict Resolution Table*, a full tabular IRD was constructed. Direction of influence for each of the affinity-pair relationships contained in the *Conflict Resolution Table* was transcribed in the *Tabular IRD of Affinity Relationships Table* (Table 14).

Table 14. Tabular IRD of Affinity Relationships Table

Tabular IRD											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**OUT**	**IN**	**Δ**
1		←	←	←	↑	←	←	←	1	6	-5
2	↑			←	↑	↑	↑	↑	5	1	4
3	↑			←	←	↑	↑	←	3	3	0
4	↑	↑	↑		↑	↑	↑	↑	7	0	7
5	←	←	↑	←				←	1	4	-3
6	↑	←	←	←			↑	↑	3	3	0
7	↑	←	←	←		←			1	4	-3
8	↑	←	↑	←	↑	←			3	3	0

Unresolved conflicts are highlighted within the table and are important to note because these conflicts were placed on "hold" to be used after the initial SID was created. In tabular form, the IRD depicted relationships that influenced each affinity (*In*: B → A and A ← B), and relationships influenced by each affinity (*Out*: A → B and B ← A)

(Turner, 2006). A numeric value resulting from subtracting the number of *Ins* from the number O*uts* was used as a numerical indicator of the relative position of each affinity within the resultant SID as illustrated in the *Tabular IRD – Sorted in Descending Order Table* (Table 15).

Table 15. Tabular IRD in Descending Order

Tabular IRD – Sorted in Descending Order of Δ											
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**OUT**	**IN**	**Δ**
4	↑	↑	↑		↑	↑	↑	↑	7	0	7
2	↑			←	↑	↑	↑	↑	5	1	4
3	↑			←	←	↑	↑	←	3	3	0
6	↑	←	←	←			↑	↑	3	3	0
8	↑	←	↑	←	↑	←			3	3	0
7	↑	←	←	←		←			1	4	-3
5	←	←	↑	←				←	1	4	-3
1		←	←	←	↑	←	←	←	1	6	-5

Tentative SID Assignments

By arranging the affinities in descending order of "delta", tentative SID positions for the affinities were then assigned in Table 16, the *Tentative SID Assignments Table*. The delta values provide a proxy of the relative "weight of influence" of one affinity toward all the others within the system. The *Primary Driver* (many *Outs,* but no *Ins*) is named as such because it has considerable influence on the other affinities, but is not affected by the other affinities. The *Secondary Driver* (more *Outs* than *Ins*) have a relative influence on other affinities, as well as from other affinities within the system. Essentially, the *Secondary Driver* was not as influential on the other affinities as the

Primary Driver, but was still a relatively strong force for influence toward other affinities compared to how many other affinities' affect it.

Pivots (*Outs* equals *Ins*; i.e., delta equals zero) are just that – a "pivot point" from which other affinities' influence fed back or are involved with many affinities concurrently. There were three *pivots* in this system; each pivot therefore had a mathematically equal weight (in terms of delta) as far as their relative positions within the system. To resolve this issue further, an examination of the *pivot* relationships illustrated by the *Tabular IRD of Affinity Relationship Table* (Table 14) indicated that affinity #6 influenced affinity #8 (6 → 8), and 8 influenced 3 (3 ← 8). Because the 3 ← 6 relationship also conflicted with 3 → 6, the logical order of the pivots was resolved in accordance with these issues as represented in the *Tabular IRD – Sorted in Descending Order Table* (Table 15); the conflicts would subsequently be reconciled during the construction of the final SID.

Table 16. Tentative SID Assignments Table

Tentative SID Assignments		
#	**Affinity Name**	**Location/Assignment**
4	Organizational Context	Primary Driver
2	Personal Impact/Outcome	Secondary Driver
6	Expectations	Pivot
8	Security of Technology	Pivot
3	Complexity	Pivot
7	Vicarious Experience/3rd-Party Influence	Secondary Outcome
5	Security of the Channel	Secondary Outcome
1	Credibility	Secondary Outcome

The *Secondary Outcomes* (more *Ins* than *Outs*) were the result of the relative influence of many more of the stronger affinities while still maintaining some degree of influence on the other affinities. A *Primary Outcome* is an affinity affected by other affinities but does not itself influence any other affinities in the system. Results indicated there were no *Primary Outcomes* (many *Ins*, but no *Outs*) in the constituents' system of perception and experience; each affinity had an affect on at least one other in the system.

Constructing the System Influence Diagram

The first step to constructing the SID was to organize the affinities in order of relative position according to the *Tentative SID Assignments Table.* Arrows were drawn as links between affinities to represent the influence between affinity-pair relationships as indicated in the *Tabular IRD of Affinity Relationships Table* (relationships inside the dotted triangle in Table 14). Figure 3, known as a *Cluttered* SID, illustrates the outcome of this process.

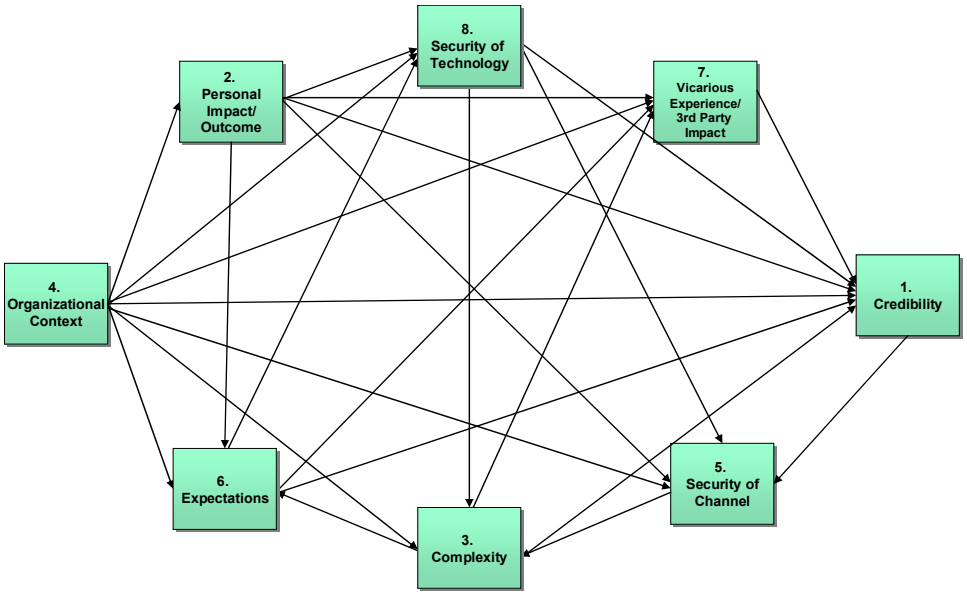

Figure 3. Cluttered SID

The *Cluttered SID* represents all the affinity-pair relationships that survived the Min/Max criterion but is generally too complex and intricate to be a very useful representation of an abstract system due to redundant links between the affinities; hence, redundancies were systematically removed. The process of removing redundant links was based on delta and SID assignments whereby direct links between affinities from the extreme left (drivers) to the extreme right (outcomes) are removed if another indirect path still provides the requisite connection between the two affinities. In other words, a direct link between the highest and lowest delta-assigned affinities was removed only if there was an alternative path (the path did not need to be a direct link) between the two affinities. For example, as depicted in Figure 4, the direct 4 → 1 link is removed because we can still depict the meaningful connection/influence of 4 → 1 by retaining the linkages between 4 → 2 → 1).

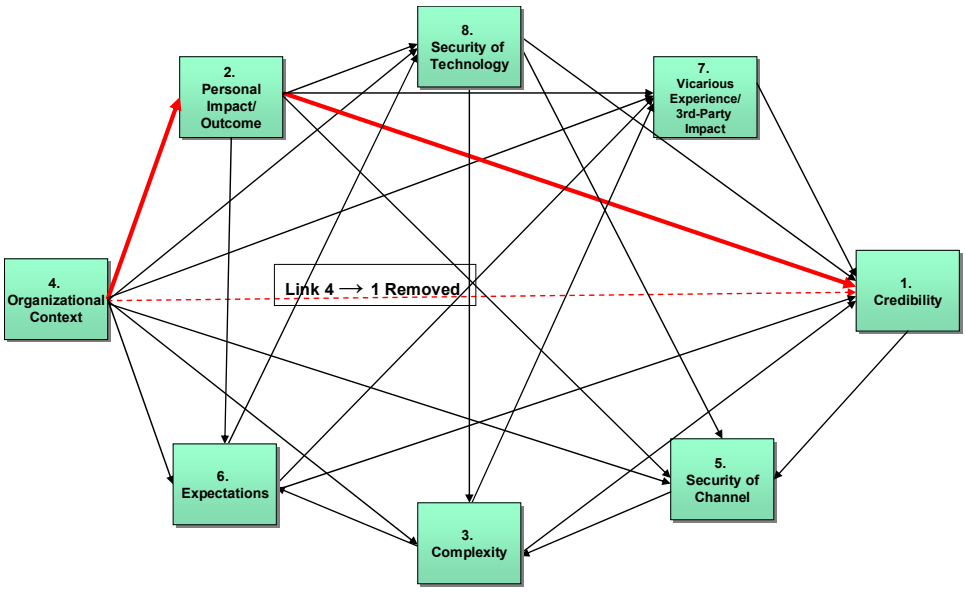

Figure 4. Removing a Redundant Link

The process continued until all redundancies were removed. The outcome of this process was the *Uncluttered SID*. At this time, the conflicts noted from Table 13 were added back into the graphical system prior to a final simplification and removal of remaining redundancies. Figure 5 depicts the Uncluttered SID with conflicts represented by arrows with dashed lines. Again, redundancies were removed via the same simplification process previously described.

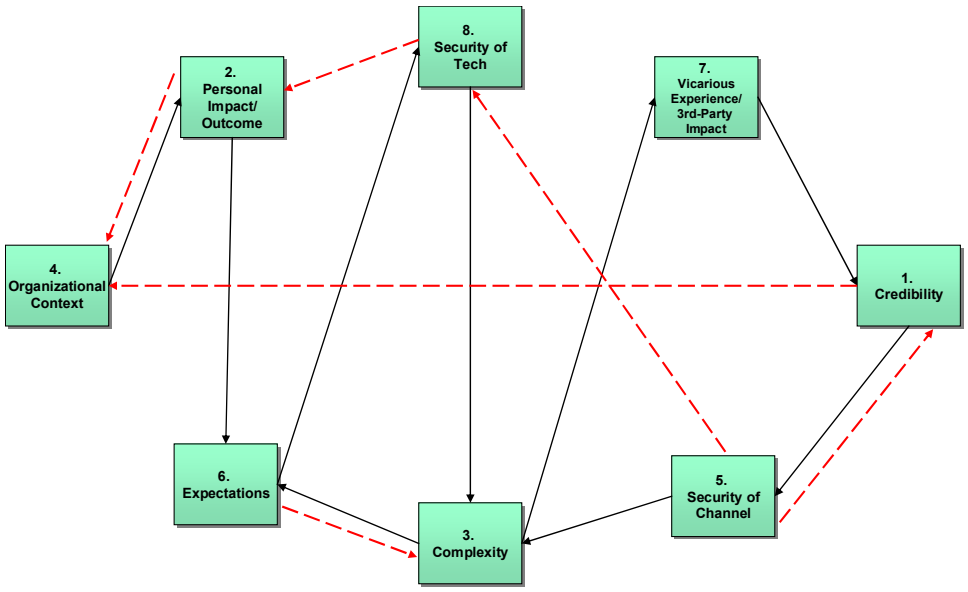

Figure 5. Uncluttered SID with Conflicts Added

The Final SID

Figure 6 represents the *Final SID* with all redundant linkages removed between system affinities. Although both the *Pareto Cumulative Frequency and Power Analysis Table* (Table 12) and the *Cluttered SID* (Figure 3) could just as well represent the system, the *Final SID* provides a parsimonious conceptual model of the problem/phenomenon as

it exists in the minds of the focus group constituents. The next chapter will discuss significant aspects of the *Final SID* as well as some observations and analyses associated with the system.

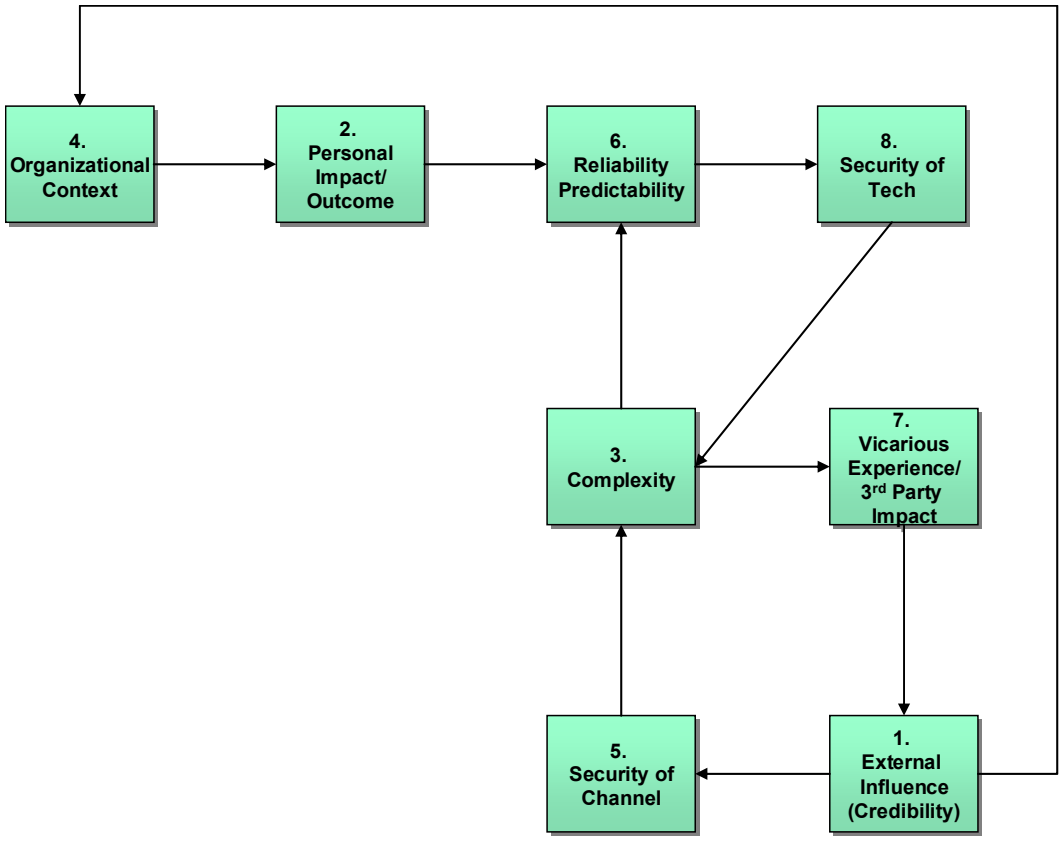

Figure 6. Final SID

CHAPTER 5: DISCUSSION AND CONCLUSION

Discussion

Based on the IQA methodology, a focus group constituency of 15 military IT professionals provided their individual perceptions, experiences, and beliefs in regards to what makes each of them suspicious of IT. Through group consensus-building, the constituents provided eight affinities or elements of suspicion and provided their individual notions of the means by which each element influenced the others. The resultant system of experience and perception provides a theoretically compelling foundation from which to explore the nature of IT suspicion because it was envisioned by those who are arguably close to the problem or phenomenon. Additional discussion regarding the nature of the final system is provided in the following sections with particular emphasis on certain noteworthy aspects of the system affinities and relationships.

Affinity-Pair Influence Relationships

Organizational Context Influence

Analysis clearly indicated *Organizational Context* was perceived as "most responsible" for all subsequent perceptions, experiences, and interpretations associated with all the other things that make us suspicious of IT. As depicted in the *Final SID*, *Organizational Context* was the primary driver of the system. Upon reflection, the "essence" of the constituents' themes and meanings associated with *Organizational Context* seemed to mirror the structural mechanisms of Adaptive Structuration Theory

(AST) (DeSanctis and Poole, 1994). According to DeSanctis and Poole, "AST focuses on social structures, rules and resources provided by technologies and institutions as the basis for human activity." (p. 125). One such structure is provided by the organizational environment (Ibid.); hence, the basis for this discussion. It is reasonable to conclude within the context of an organization like the Air Force, with so many embedded, ingrained, explicit, and implicit organizational influences, that members' actions, perceptions, and experiences are highly influenced by that organizational environment. Indeed, it is the nature of the military, as an institution of traditions, high standards, and professionalism that creates a culture of conformity to rules and regulations; therefore, the contextual structures (such as the focus group's "policies") of this particular organization naturally exerted a strong influence on the focus members' actions and thought processes.

AST also suggests that IT provides social structures in the form of *structural features* (i.e., the rules, resources, and capabilities) and a *spirit* (i.e., the general intent or use) underlying the features of a system (DeSanctis and Poole, 1994). The appropriation or adaptation of social structures by organizational members influences the way in which members identify with and implement such structures. Hence, contextual structures can also inform which IT structures or *spirit* is appropriated. The structures inherent of the organization, whether they were the technology, policies, management decisions, or the culture of the organization strongly impacted user perceptions of the IT used in the organization. In this light, *Organizational Context* provides for perceptual mechanisms similar to those described for situationally-aroused suspicion (Levine and McCornack, 1991; Fogg and Tseng, 1999) because the context of the Air Force organization

essentially was the situation/environment in which the constituents' suspicion of IT would be aroused.

The notion of a suspicious predisposition is also a relevant facet of the organizational context as described the focus group. As mentioned in the literature review, Generalized Technology Suspicion (GTS) is similar to Levine and McCornack's (1991) Generalized Communicative Suspicion (GCS). Recall that GCS is an inherent belief that all incoming communication behaviors from others are deceptive (Ibid.), whereas GTS is a perception that there is reason to be suspicious of all technology. Although, not all people are predisposed to GTS, it does imply a general assumption people make about technology (Fogg and Tseng, 1999). In the case of this research, the fact that the constituents were IT professionals in the Air Force may have attributed to a generalized predisposition toward GTS (Conti et al., 2005; Hollebeek and Waltzman, 2004). Indeed, the constituents' knowledge and training of IT security and defense of military networks, and the fact they were all students of a graduate program for which topics such as IT security vulnerabilities are discussed and researched, likely contributed to such a predisposition. Further discussion of the impact/influence that the *Organizational Context* has on the other affinities is provided in several of the individual affinity discussions that follow.

Personal Impact/Outcome Influence

The *Final SID* revealed *Personal Impact/Outcome* as a having a relatively strong influence on the other affinities, as opposed to the other affinities influence on it – with the exception of the previously discussed *Organizational Context*. Hence, constituents

felt their personal experiences had a strong impact on their perceptions of the IT they have used. It is not surprising that first-hand 'experience' is an influential element of the system because it solidifies a person's perceptions via repeated interactions with IT (Fogg and Tseng, 1999). The *Organizational Context* was certainly an influence on the constituents' inputs for this affinity. Indeed, the personal experiences of the constituents could have come from experiences outside of work; however, evaluation of the reported data on the ARTs revealed a majority of constituent inputs were derived from personal impact and experiences generated in the workplace. For example, the failure of implementing a new system led to the loss of an individual's work-related data in which he had invested a great deal of time and effort.

Expectations

Several inputs regarding personal experiences were quite similar and indicated a general tendency towards *negative* rather than *positive* experiences and perceptions. Therefore, findings suggest negative user experiences with IT lead to IT suspicion. The basis for this finding seems to stem from the notion that experiences lead to general expectations (Muir, 1987). Hence, the *Personal Impact/Outcome → Expectations* relationship aligns with the findings of previous studies (Muir, 1987; Fogg and Tseng, 1999; Flechais et al., 2006).

It was also clear from constituent inputs that they were referring to expectations they had about the technology per se as opposed to expectations of information residing on the technology or the use of technological communications channels. Specifically, constituents noted that reliability and predictability of technology, such as a computer,

resulted in generalized expectations of how a computer should behave. Furthermore, the negative connotation of the overall constituency's inputs indicated that certain *expectations* are user-established standards and that only when deviations to user expectations occur would a user become suspicious of the technology.

Security of the Technology

Constituents noted their experiences led to general expectations such as reliability and predictability of IT. Closely related to the general expectations reported above (and an affinity that could potentially be generalized as a user expectation in its own right) is the *Security of the Technology*. Constituent inputs indicated that user expectations of security issues are extremely important and that technology in general was perceived or experienced as not fully secure. Specifically, the constituents referred to the *Security of the Technology* affinity as the "lack of" security, and that this lack of security invoked suspicion. Hence, constituent expectations were that the security aspects of technology are generally deficient. Again, the *Organizational Context* was found to influence this affinity as the nature of the constituents' studies and research, which included topics pertaining to security issues with IT, undoubtedly affected their perceptions (or expectations) regarding IT security in general, as well as simply a general increase in the awareness of IT-security related issues.

Complexity

Perceptions and experiences regarding *Security of the Technology* influenced the way constituents thought about the *Complexity* of IT. Recall from the previous chapter's discussion about complexity that difficulties in usage were directly related to the overall

complexity of a piece of IT. The previously discussed elements of suspicion such as dispositional inferences, uncertainty, and self-efficacy certainly seemed to be at the heart of this relationship.

For example, constituents posited that the complexity of the technology actually affected the usability of the system. However, usability of a technology is a perception generated via a dispositional inference made on the technology (Murphy et al, 2003; Rozanski and Haake, 2003); hence, it stood to reason that some constituents expressed the fact that "if I think a technology is too complex, then I will avoid using it." Another aspect of this relationship was that notion that security added an element of uncertainty to the technology where all features or characteristics of the security may be unknown to the user. Such uncertainty may further be responsible for the contributions of self-efficacy perceptions to IT suspicion. Specifically, in the face of additional security features that increase the complexity of a piece of technology, the mounting uncertainty would prompt a user to question his/her knowledge and abilities. As Gross and Rosson (2007) observed, perceptions of self-efficacy can contribute to overall suspicion.

Security of the Channel

Recall that the original "Privacy" affinity seemed to center on the more general notion of *Security of the Channel* upon which information was sent, including such subjects as online transactions and the use of various channels such as the Internet, cell phones, email, and instant messaging for conducting such transactions. Hence, information security was an essential part of this category because the lack of security of the channel may lead to manipulated or lost information. As indicated in the literature

review, the media used in communication intensifies our concerns about the integrity of the channel (Riegelsberger, et al., 2005). These concerns about the *Security of the Channel* therefore result in user suspicion of the channel (Shechtman and Horowitz, 2003). Indeed, Constituents expressed their doubts when it came to the security of the technologies used to communicate information while blaming IT companies for providing defective products and services. Therefore, user perceptions of the *Security of the Channel* were clearly influenced by notions of *Credibility* because constituents felt IT companies do not provide for a degree of security in their products and services that users expect in order to protect one's privacy.

Further Analysis and Abstractions

External Influence Affinity

During the process of analyzing and interpreting the model it became clear that the *Vicarious Experience/3rd Party Impact* and *Credibility* relationships were tightly coupled, perhaps even elements of the same larger affinity or concept. The underlying principle for this assertion is the notion of *external influence* on a user. External influence comes from information provided via a third-party; however, as discussed in the literature review, third-party information is also subject to a credibility judgment by the user of such information (Fogg and Tseng, 1999). Essentially, a credibility judgment can be influenced externally by third-party information – exactly the relationship articulated here in the final model of IT suspicion. Certainly, third-party information could come directly from other users, TV, radio, and websites to mention a few; however, users may also experience such information vicariously. For example, constituents did not personally

experience unsafe events as a result of using IT; thus, their notion of "safety" as it related to IT suspicion was actually based on the vicarious experiences and reports of others.

In addition, the companies responsible for IT themselves may be a source of external influence through their reputation, products and services. From a social context, a credibility judgment is an evaluation of another person's trustworthiness (Burgoon et al., 1996). Constituents seemed to apply this rule to IT companies whereby constituents felt the *Credibility* of IT companies affected their perceptions of those companies' products and services. The literature review suggested that a user's perceived suspicion of the source (i.e., an IT company or other users) affects the perceived credibility of the information provided by that source (Ibid.). Hence, credibility and suspicion mutually affect each other.

In light of these observations, the *Vicarious Experience/3rd Party Impact* affinity was combined with the *Credibility* affinity to form a conceptually more complex but still meaningful (in terms of the original two affinities) *External Influence* affinity. The rationale for this decision was grounded in the various concepts and issues discussed in the literature review, as well as the findings themselves. In particular, suspicion may be influenced by negative information from third-parties. However, third-party information must be provided by credible sources – at least credible as perceived by the user. Credibility is an evaluation of trustworthiness and expertise (Fogg & Tseng, 1999). In this case, the perceived trustworthiness and expertise of IT companies, their products and services, affected a company's reputation – in other words, a credibility judgment (Ibid.).

A modified version of the *Final SID* is depicted in Figure 7 which incorporates this affinity-pair abstraction. Note that that the general proximity and connectivity

between the remaining system affinities has not been altered; however, by representing the tight coupling and conceptual overlap of the two affinities into a single, more meaningful affinity, the model itself is actually more informative in light of existing suspicion theory and research. A miniature graphic of the *Final SID* is provided to illustrate the difference between the *Final SID* and the *Modified Final SID*.

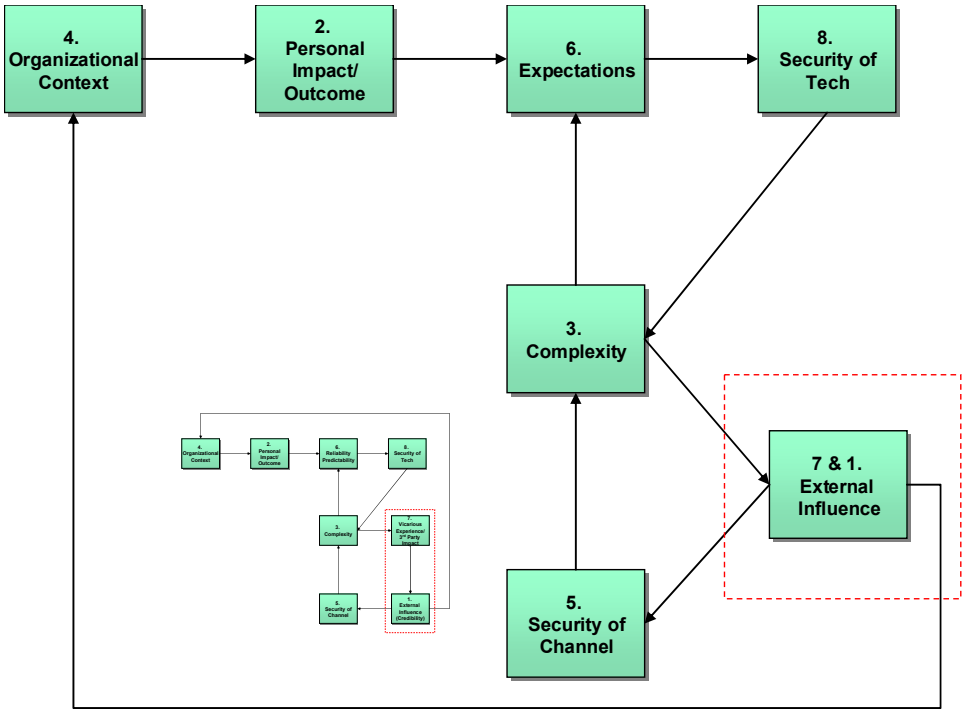

Figure 7. Modified Final SID

External Influence → Organizational Context

It was important to address the relationship between *External Influence* and *Organizational Context* because this relationship essentially "closed the loop" on the entire system of perception and experience regarding suspicion of IT. What this implied is that such suspicion is not ultimately deterministic – experiences and perceptions of

issues “downstream” in the system can in fact propagate their influence back through the system to ultimately change or influence the perceptions and experiences of the various “upstream” or driving issues associated with IT suspicion. In particular, the data concerning the connections between *affinity 7/1, External Influence* and *affinity 4, Organizational Context,* indicated a conflict; the constituents’ experiences and perceptions between the two were therefore ambiguous and difficult to articulate definitively in one direction or another.

On the one hand, *Organizational Context* was perceived to directly influence perceptions of credibility in that constituents felt the organization they were part of sometimes made decisions that conflicted with user needs, perceptions, and expectations. Constituent inputs suggested policies that led to either extreme constraint or an overreaction to adapt or use IT (such as the example provided regarding the implementation of a redundant system). However, it was also the case that experiences and perceptions of credibility, which were primarily the culmination of the impacts and influences from all the other factors in the system, could still impact or alter the nature and perceptions of the clearly influential organizational context. For instance, IT companies want to establish credibility for themselves, and the way they do this is to provide products and services that will provide positive user experiences (Binstock, 1999). Although this suggests an example of an organization outside of a user’s immediate context or workplace, the same holds true for a user’s organization in attempts to establish member credibility within the organization. Hence, the credibility established within an organization facilitates positive user perceptions of the context of the organization (such as the way it implements its IT policies).

This final feedback loop that interconnects all the factors within the system suggests that AST-like mechanisms of enforcement and reinforcement were at work in the minds and experiences of the constituents in relation to suspicion of IT. For example, the appropriation of certain social structures (i.e., structural features and spirit) clearly influenced user experiences and expectations of IT within the context of use (DeSanctis and Poole, 1994). However, constituent inputs suggested that conflicts exist between user needs and corporate or organizational interests indicating a potential mismatch of these structures or the possibility of misappropriating the structures inherent in IT for use within the organizational context. The result of these experiences and potential misappropriations (such as constituent concerns with organizational policies) could thus feed back to affect changes in the *Organizational Context* in such a way that user attitudes and adoption of the technology were altered again.

Ambiguous Relationships

The type of relationship that exists when conflicts are not resolved is manifested into what are referred to as *Ambiguous Relationships* (Turner, 2006). The *Final SID* depicted two such relationships which were ultimately reconciled into a pair of *Feedback Loops*. A simple version of this type of relationship with three affinities (it could be more) is illustrated in Figure 8. What is interesting about this "loop" is the fact that several arguments could be made as far as which affinity influences another. For example, if an argument exists that C → A, then one would indicate A influences B, and B influences C; hence, A indirectly influences C (through B). Therefore, if B is removed from the system, then the C → A and A → C affinity-pair relationships are essentially

equally supported hypotheses (Ibid.). Thus, the feedback loops are useful representations of ambiguity of thought on the part of the constituents because they allow us to articulate a situation in which experiences or perceptions of one affinity both influence, and are influenced by, other affinities within the same system.

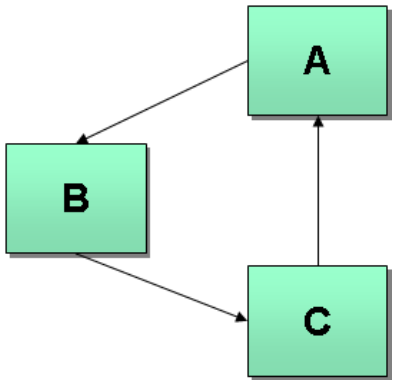

Figure 8. Sample Feedback Loop (Source: Turner, 2006)

The *Modified Final SID* (Figure 7) illustrates that a *Feedback Loop* existed among the *Complexity, Expectations, and Security of the Technology* affinities. These three affinities were also *Pivots* within the model as illustrated in the *Tabular IRD of Affinity Relationships* (Table 14). *Pivots* are essentially a "pivot point" from which other affinities' influence within the system feed back, into, or involve many other affinities concurrently. These three affinities, because their deltas each equaled zero, had equal weight as far as their position to each other within the system. Examination of the content and nature of the relationships between the affinities themselves indicated that this feedback loop centered on constituents' perceptions of suspicion directly relative to the "technology." Hence, it appeared constituents found it difficult to distinguish which element (i.e., expectations, security of the technology and the complexity of technology) invoked a higher degree of suspicion.

Another *Feedback Loop* existed among *Complexity, External Influence, and Security of the Channel* affinities. Examination of these affinities revealed that elements of third-party and technological influence were also common to each. For instance, it was previously discussed that information from third-parties may lead to suspicion of IT. The complexity and security of the technology or the channel may also lead to lost, manipulated, or simply wrong information. Hence, information from third-parties may not be accurate which would then lead a user to become suspicious of the information. Credibility judgments are also difficult to render when the channel from which the information was communicated is suspected to have inadequate security.

Interestingly, *Complexity* links the two inner feedback loops together. Constituents defined complexity on the basis of an IT systems' level of difficulty to implement or use; therefore, complexity denotes a user's uncertainty about a technology. Literature suggests that uncertainty is an element of suspicion (Kee and Knox, 1970) and that those users who lack the complete knowledge and experiences of an IT system are uncomfortable about using it (de Vries et al., 2003); these same connections were apparent in the constituent inputs. A person's own perceptions about his/her own abilities (i.e., self-efficacy) also affect his/her perceptions about the complexity of technology (Compeau et al., 1999); again as one individual indicated, "If it's too difficult, then I probably won't use it."

Simplifying the Model

By continuing the logic presented in the discussions above concerning the multiple individual affinity-pair relationships and feedback loops, a further simplification

and abstraction of the system became evident. As depicted in Figure 9, four conceptual zones related to suspicion of IT are proposed. The name given to each zone reflects its general theme or meaning. Connections made to the suspicion process in the aforementioned literature review are provided in the separate discussions of each zone.

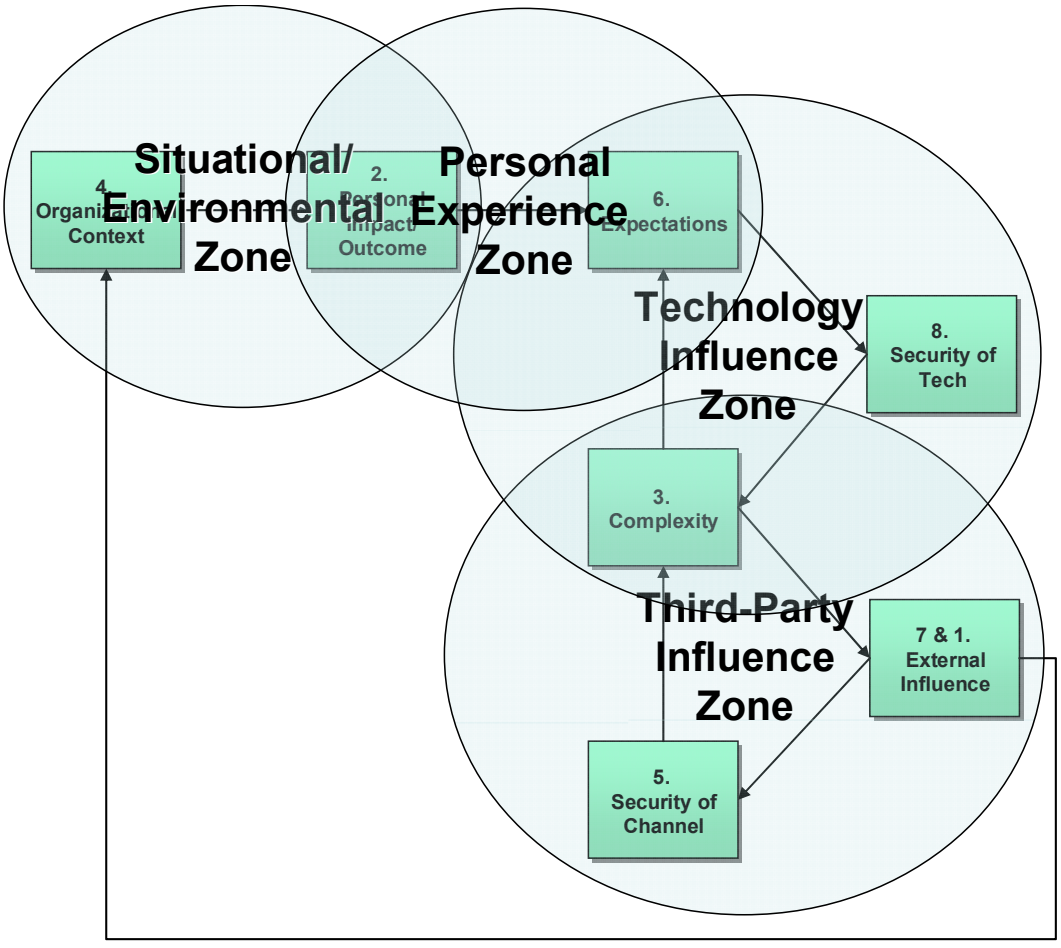

Figure 9. SID with Four Zones

Situational/Environmental Zone

Organizational Context and *Personal Impact/Outcome* are included in this zone. In comparing the relationship between these affinities it was evident that the situation or environment a user was part of had a considerable impact on whether a user became suspicious of IT. Hence, the elements of suspicion indicative of this zone seemed to mirror the issues associated with *Situationally-Aroused* suspicion as discussed in the literature review. It was no surprise that the constituents, because they were all IT professionals in the military, were affected by the situation/environment they were subject to. However, the situation/environment also facilitated a users' ability to obtain unique experiences such as defending an organizational network, or managing information systems.

Personal Experience Zone

Personal Impact/Outcome and *Expectations* were part of this zone because experiences lead to the development or reinforcement of various expectations. As suggested from the previous literature review, *Expectations* are a principle element of suspicion (Binstock, 1999; Bottitta and Felici, 2006; Burgoon et al., 1996; Bradley, 1998; Flechais et al., 2006; Muir, 1987). However, a user's actual experiences with IT eventually lead to a level of general expectation of the technology (Muir, 1987; Fogg and Tseng, 1999; Flechais et al., 2006). Constituents felt that the reliability and predictability of a system was important, because it offered a level of comfort for them from which they could base subsequent perceptions of that system's trustworthiness. Individuals noted their bad experiences, such as "bugs in operating systems" and "excessive

downtime due to a failure in the system" to mention a few. The negative connotation of the constituent inputs suggests that deviations to user expectations of the technology lead to user suspicion of that technology – an observation previously discussed.

Technology Influence Zone

Expectations, Security of the Technology, and *Complexity* each referred to the subject "Technology" in the minds of the constituents. These three affinities were subject to a series of ambiguous relationships that ultimately formed a feedback loop. Hence, each affinity had an equal weight of influence on the other within the system. It is within this feedback loop that the suspicion elements of *expectations, dispositional inferences, uncertainty, and self-efficacy* are likely responsible for the many perceptions and experiences associated with these ambiguous relationships. Most significant to discuss within this zone is the *Complexity* affinity, because it essentially tied the two previously mentioned feedback loops in the system.

In particular, constituents felt that IT that is difficult to use constitutes user perceptions of the complexity of the technology. Hence, constituents not knowingly mentioned that they were essentially making a dispositional inference toward the technology. Some individuals went as far as to say that if the technology looked complex then it probably was, and that it would discourage users from adapting that technology. However, the majority of constituent inputs suggested that a "learning curve" exists especially when it comes to new technology – an example provided by the group was the excessively large user manuals that accompany many IT products. Therefore, constituents expressed their notions of uncertainty of the IT based on their abilities to comprehend all

the intricacies that are inherent of an IT system; hence, the argument of self-efficacy comes into play.

Third-Party Influence Zone

The *Third-Party Influence Zone* included *Complexity, Security of the Channel,* and the combined affinity *External Influence*. Similar to the *Technology Influence Zone*, the affinities in the *Third-Party Influence Zone* were comprised of ambiguous relationships that formed a feedback loop. What this suggested was that third-party information can come from many different sources including other users, TV, radio, and websites just to name a few; and that such information could also come indirectly or vicariously from these same sources. As mentioned in the literature review, third-party information can arouse user suspicion (Stiff et al., 1992) and that the aroused suspicion can be increased or decreased by further interaction. However, a user must determine credibility of the information or the source, even when there are questions that arise regarding the security of the communications channel used to convey the information. Both of these factors were found to further fuel one's perceptions and experiences of *Complexity*.

Interpretation of the Final Model

So what does suspicion of IT look like? The *Simplified Final SID* represents a cognitive model of the IT suspicion process and may be implemented as such. In relating the model to the concepts from the literature review, each of the four zones represents an axis for initiating or resolving a suspended judgment. This research demonstrated that suspicion of IT truly is a complex process and the system model has provided greater

fidelity as to what specific issues are considered or negotiated; and how, as the suspicion process plays out. To clarify this point, a brief review of the suspicion process is necessary. First, the suspicion process involves a suspended judgment and the final outcome of this judgment is a decision to trust or not to trust (i.e., a trust-decision). The suspended judgment is resolved through a process consisting of three sequential stages: categorization, characterization, and correction (Gilbert et al, 1988). These three stages are respectively summarized and defined as identify, anchor, and adjust. Therefore, within the model obtained in this study, each zone represents a cognitive subject area in which a suspended judgment about IT occurs. More specifically, each zone indicates an area for which an IT user makes a trust-decision.

Based on the degree of influence and interconnection as depicted by the model, each zone must also be resolved prior to moving on to the next, though the resolution of issues in a subsequent zone may feed back to impact or change perceptions and experiences about prior issues that will further influence trust-decisions. Within each zone are the affinities or suspicion elements from which a user identifies, anchors, and adjusts his decision. For example, in the *Situational/Environmental Zone*, a suspended judgment would take into account both *Personal Impact/Outcome* and *Organizational Context* in making a trust-decision. As one would expect, a military member who is an IT professional and perhaps working in area of network defense would be more susceptible to suspicion because he/she is highly influenced by the nature of his/her job. However, the *Personal Experience Zone* is also an area of suspended judgment connected to the *Situational/Environmental Zone.* Hence, the system identifies that these two zones are highly coupled.

Interestingly, both the *Technology* and *Third-Party Influence Zones* are representative of ambiguous relationships. The reason why the suspicion process involves a wealth of cognitive resources is because of the constant anchoring and adjusting of multiple hypotheses as was mentioned in the literature review discussion (Fein, 1996; Fein et al., 1990; Hilton et al., 1993; Gilbert et al., 1988; Tversky and Kahneman, 1974; Quattrone, 1982). In reference to the suspicion process, these ambiguous relationships, and the even more compelling overall feedback loop of the system, represents the additional complexities involved in resolving a suspended judgment, and can illustrate or account for how and why one might remain in a state of suspended judgment without ever reaching a resolution. For these reasons, the suspicion process associated with IT may not always be a quick decision; it may last a relatively long time based on the difficulties a user encounters with the numerous suspended judgment processes a user must cognitively overcome to make a final trust-decision.

Limitations and Recommendations for Future Research

A limitation to this study exists in the selection of the focus group members, specifically the representative size and demographics. Specifically, a focus group was used to obtain the data from constituents who, according to the principle researcher, are closest to the problem/phenomenon. However, the overriding research question for this study was: *What is the nature of user suspicion toward IT?* The question implied a broad population of IT users; therefore, the relatively narrow sampling of focus group participants in this study may not represent the perceptions, realities, or lived experiences of an entire population of IT users. The cognitive dimension of the information

environment is a critical area of research in light of the increasing use of IT in the military and globally.

Hence, although this study created a model indicative of perceptions and experiences of some IT professionals, it would be interesting and theoretically relevant to obtain results from a constituency of typical IT users. Perhaps studies focusing on gender or cultural differences would create a different model as well. However, to truly obtain results of a majority population, a larger and more diverse constituency should facilitate a representative model of the typical IT user. Furthermore, a more inclusive IQA approach to include interviews or perhaps multiple focus groups would create a more robust data set than that obtained for the current research.

Clearly, *Organizational Context* was the primary influence on the rest of the system. Perhaps a non-military constituency of IT professionals who were not managers per se would not be as strongly influenced by the context of their organization? Would non-professional users of IT even conceive the notion of an organizational context? If not, then what would become the primary driver in the system? Another limitation to this study is that the model may not reflect the system as it pertains to specific IT jobs or tasks. For example, a group of network security professionals may have a different mental model when compared to a software engineer or interface designer. Perhaps a group of computer scientists and engineers would mirror a system in which *Complexity* would not be part of a feedback loop. A potentially more intriguing recommendation for future research takes this notion of suspicion and examines it from the attackers' vantage point…*what would the system look like for a group of computer hackers?*

More specific concerns in the execution of the methodology included the room in which the focus group was held and the time allocated for the meeting. During the meeting, some constituents expressed their dissatisfaction with the temperature of the room; however, temperature controls were not available. It is possible that physical discomfort on the part of some participants have led to the precipitous naming of the affinities or *axial coding,* and even more so the *theoretical coding* of affinity-pairs to establish influence relationships, which was the last task the constituents were asked to do. The time allocated as addressed to the focus group prior to the meeting was 2 ½ hours. Although the meeting lasted a little over 2 hours, perhaps if the constituents were told 3 hours, they would have allocated more time in their busy schedules and not have felt rushed, especially toward the end of the meeting when the *theoretical coding* task was accomplished.

Finally, a modified version of the IQA methodology was implemented such that the sole use of the focus group was employed for collection of data. In a more typical IQA study, individual interviews with constituents are conducted some time after the focus group whereby further examination and interpretation of the affinities and the *theoretical coding* is accomplished to better understand the nature and contents of the obtained system (Turner, 2006). In the course of this research, examination and follow-up interpretation of the data was conducted by the principle researcher only, thus introducing the possibility of researcher bias in the construction and interpretation of the resultant affinities and system of perception and experience.

Implications for the Air Force

The implications of this study and resultant system of IT suspicion may be used as a conceptual framework from which a robust IT suspicion model or training paradigm could be developed and implemented by organizations as part of their network protection practices or Information Assurance programs. Certainly, the *Situational/Environmental Zone* is a significant portion of the model, because it includes the primary and secondary drivers of the system. Hence, the context of the organization should focus on the needs of the user to ensure the structures in the organization relevant to the use of IT are appropriated correctly. A level of agreement between users and management in the appropriation of structures inherent to IT and the organizational environment should also facilitate IT use; thus providing the necessary user experiences to encourage further use and development of positive affect and perceptions surrounding the IT itself.

The *Technology Influence Zone* is also an area for which training should focus. The model indicates that *Complexity* is important because it is a central link between the two ambiguous relationships. *Complexity* is an issue central to users' concerns about IT and thus within their suspicion process. The importance of this linkage suggests that by eliminating or at least decreasing perceptions of IT complexity, a user's suspicion process of resolving a suspended judgment might facilitate a quicker trust-decision. The implication of such gains in resolution speed suggest that complexity is a key consideration in creating a more effective and rapid OODA loop than that of our adversaries (AFDD 2-5; Gibb, 2000). It is likely that adequate training and hands-on experience would mitigate a user's uncertainty about technology and provide for greater confidence about IT necessary to make quicker and better decisions.

Furthermore, the *Technology Influence Zone* indicates that users' expectations and experiences are that the technology is not secure and that it is very complex. This area of the model suggests that training of IT users for the purposes of detecting of deception or attempts to hack into our computers and networks should focus on both the security-related issues of the technology as well as demystifying the complexity of the technology itself. Such training should also focus on the issues associated with the *Third-Party Influence Zone.* For instance, a general awareness of the security issues surrounding various communication channels (*Security of the Channel*) were observed to be key to the processes by which users become suspicious of IT; focus on such issues may perhaps sensitize users to better detect computer and network attacks.

Conclusion

The purpose of this study was to address the problem/phenomenon of IT user suspicion and to answer the question at the heart of this investigation: *What is the nature of user suspicion toward IT?* The IQA methodology allowed for a flexible but disciplined approach to generating and analyzing data appropriate for answering that research question. The results of this study show that user suspicion toward IT is a very complex cognitive process that exists in the minds of IT users. However, analysis also showed that a user's situation or environment vastly affects the outcome of his/her suspicion process. In addition, a user's personal experiences, third-party information, and the technology itself can affect a user's suspicion process. The obtained model of IT suspicion also illustrates the complexities and connections between the psycho-social and technology-related perspectives of suspicion, suggesting that the nature of suspicion toward IT is

indeed rooted in the same interpersonal suspicion mechanisms and processes inherent in social interactions.

BIBLIOGRAPHY

ACM Special Interest Group on Computer-Human Interaction [ACM SIGCHI] (2008). Excerpt from webpage. n. pag. http://sigchi.org/. January 21, 2008.

Baltes, B. B., Dickson, M. W., Sherman, M. P., Bauer, C. C., & LaGanke, J. S. (2002). Computer-mediated communication and group decision making: A meta-analysis. *Organizational Behavior and Human Decision Processes*, 87(1), 156-179.

Bandura, A. (1986). *Social Foundations of Thought and Action: A Social Cognitive Theory*, Englewood Cliffs, NJ, Prentice Hall.

Bickmore, T. W. & Picard, R. W. (2005). Establishing and maintaining long-term human-computer relationships. *ACM Transactions on Computer-Human Interaction,* 12(2), 293-327.

Binstock, A. (1999). New mantra: Usability. *InformationWeek,*(751), 1A-10A. Retrieved January 21, 2008, from: ABI/INFORM Research database. (Document ID: 44522359).

Biros, D. P. (1998). *The effects of truth bias on artifact-user relationships: An investigation of factors for improving deception detection in artifact produced information.* PhD dissertation. Florida State University, Tallahassee, FL (ADA350908).

Biros, D. P., George, J. F., & Zmud, R. W. (2002). Inducing sensitivity to deception in order to improve decision making performance: A field study. *MIS Quarterly*, 26(2), 119-144.

Bonito, J. A., Burgoon, J. K., & Bengtsson, B. (1999). The role of expectations in human-computer interaction. In *Proceedings of the International ACM SIGGROUP Conference on Supporting Group Work*, (Phoenix, AZ, November 14-17, 1999). GROUP '99. ACM, New York, NY, 229-238.

Bottitta, S. & Felici, M. (2006). Understanding and learning trust: A review, characterization and tool. Retrieved December 10, 2007, from: http://homepages.inf.ed.ac.uk/mfelici/doc/Bottitta_Felici_trust.pdf

Burgoon, J. K., Buller, D. B., Ebesu, A. S., White, C H., & Rockwell, P. A. (1996). Testing interpersonal deception theory: Effects of suspicion on communication behaviors and perceptions. *Communication Theory*, 6(3), 243-267.

Bradley, J. (1998). Human-computer interaction and the growing role of social context. *American Society for Information Science. Bulletin of the American Society for Information Science, 24*(3), 18-19. Retrieved January 20, 2008, from: ABI/INFORM Research database. (Document ID: 26830784).

Buller, D. B. & Burgoon, J. K. (1996). Interpersonal deception theory. *Communication Theory*, 6, 203-242.

Carlson, J. R., George, J. F., Burgoon, J. K., Adkins, M., & White, C. H.. (2004). Deception in computer-mediated communication. *Group Decision and Negotiation,* 13(1), 5-28. Retrieved March 5, 2008, from: ABI/INFORM Research database. (Document ID: 526559451).

Compeau, D., Higgins, C. A., & Huff, S. (1999). Social cognitive theory and individual reactions to computing technology: A longitudinal study. *MIS Quarterly*, 23(2), 145-158.

Conti, G., Ahamad, M., & Stasko, J. (2005). Attacking information visualization system usability overloading and deceiving the human. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, (Pittsburgh, PA, July 06-08, 2005). SOUPS '05, vol. 93. ACM, New York, NY, 89-100.

Dassonville, I., Jolly, D., & Desodt, A. M. (1996). Trust between man and machine in a teleoperation system. *Reliability Engineering and System Safety*, 53, 319-325.

Department of Defense. (1996). *Joint Doctrine for Military Deception,* [JP 3-58]. Chairman of the Joint Chiefs of Staff, Washington D.C. Retrieved August 31, 2007, from: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_58.pdf

Department of the Air Force. (2005). *Information operations,* [AFDD 2-5]. Air Force Doctrine Document 2-5, Washington: HQ USAF. Retrieved August 28, 2007, from: https://www.doctrine.af.mil/Main.asp

Department of Defense. (n.d.). *Enabling net-centric operations,* [DoD CIO, Brochure]. DoD Chief Information Officer. Retrieved March 13, 2007, from: http://www.dod.mil/cio-nii/docs/Enabling_NCO_Brochure.pdf

Department of Defense. (2000). *Joint vision 2020,* [JV 2020]. Chairman of the Joint Chiefs of Staff. Washington: GPO. Retrieved August 31, 2007, from: http://www.dtic.mil/jointvision/jv2020.doc

Department of Defense. (2006). *Information operations,* [JP 3-13]. Chairman of the Joint Chiefs of Staff, Washington D.C. Retrieved August 6, 2007 from: http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf

DePaulo, B. M., Malone, B. E., Lindsay, J. J., Muhlenbruck, L., Charlton, K., & Harris, C. (2003). Cues to deception. *Psychological Bulletin*, 129(1), 74-118.

DeRosis, F., Castelfranchi, C., & Carofiglio, V. (2000). *On various sources of uncertainty in modeling suspicion and how to treat them.* Retrieved May 14, 2007, from: http://www.istc.cnr.it/T3/download/aamas2000/DeRosis-et-alii.pdf

DeSanctis, G., Poole, M. S. (1994). Capturing the complexity in advanced technology use: Adaptive structuration theory. *Organization Science*, 5(2), 121-147.

Deutsch, M. (1958). Trust and suspicion*. Journal of Conflict Resolution*, 2(4), 265-279.

de Vries, P., Midden, C., & Bouwhuis, D. (2003). The effects of errors on system trust, self-confidence, and the allocation of control in route planning. *International Journal of Human-Computer Studies,* 58(6), 719-735.

Druckman, D., & Bjork R. A. (Eds.) (1991) In the mind's eye: Enhancing human performance. National Research Council (U.S.) Committee on Techniques for the Enhancement of Human Performance. Washington, DC. National Academies Press.

The Economist (2007). The trouble with computers. [Electronic Version] T*he Economist, 384*(8545), 20. Retrieved November 16, 2007, from: ABI/INFORM Research database (Document ID: 1331981401).

Elaad, E. (2003). Effects of feedback on the overestimated capacity to detect lies and the underestimated ability to tell lies. *Applied Cognitive Psychology*, 17, 349-363.

Fein, S. (1996). Effects of suspicion on attributional thinking and the correspondence bias. *Journal of Personality and Social Psychology*, 70(6), 1164-1184.

Fein, S., Hilton, J. L., & Miller, D. T. (1990). Suspicion of ulterior motivation and the correspondence bias. *Journal of Personality and Social Psychology*, 58(5), 753-764.

Flechais, I., Riegelsberger, J., & Sasse, M. A. (2005). Divide and conquer: the role of trust and assurance in the design of secure socio-technical systems. In *Proceedings of the 2005 Workshop on New Security Paradigms*. (Lake Arrowhead, CA, September 20-23, 2005). NSPW '05. ACM, New York, NY, 33-41.

Fogg, B. J. & Tseng, H. (1999). The elements of computer credibility. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: the CHI Is the Limit* (Pittsburgh, PA, May 15-20, 1999). CHI '99. ACM, New York, NY, 80-87.

Gambetta, D. (1988). Can we trust? In D. Gambetta (Ed.), Trust: Making and breaking cooperative relations. 213-238. Cambridge, MA: Basil Blackwell.

George, J. F. & Carlson, J. R. (1999). Group support systems and deceptive communication. In *Proceedings of the Thirty-Second Annual Hawaii International Conference on System Sciences-Volume 1* (January 05-08, 1999). HICSS. IEEE Computer Society, Washington, DC, 1038.

George, J. F., Marett, K., & Tilley, P. (2004). Deception detection under varying electronic media and warning conditions. In *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (Hicss'04) - Track 1 - Volume 1* (January 05-08, 2004). HICSS. IEEE Computer Society, Washington, DC, 2.

Gibb, R. W. (2000). *A theoretical model to attack the enemy's decision-making process*. Paper submitted to the Faculty of the Naval War College, Newport, RI. (ADA378602).

Gilbert, D. T. (1991). How mental systems believe. *American Psychologist*, 46(2), 107-119.

Gilbert, D. T. & Jones, E. E. (1986). Perceiver-induced constraint: Interpretations of self-generated reality. *Journal of Personality and Social Psychology*, 50(2): 269-280.

Gilbert, D. T., Pelham, B. W., & Krull, D. S. (1988). On cognitive busyness when person perceivers meet persons perceived, *Journal of Personality and Social Psychology*, 54(5), 733-740.

Gilbert, D. T., Tafordi, R. W., & Malone, P. S. (1993). You can't not believe everything you read. *Journal of Personality and Social Psychology*, 65(2), 221-233.

Giordano, G., Stoner, S., Brouer, R., & George, J. (2007). The influences of deception and computer-mediation on dyadic negotiations. *Journal of Computer-Mediated Communication*, 12(2), 362-383.

Grabner-Kräuter, S., Kaluscha, E. A., & Fladnitzer, M. (2006). Perspectives of online trust and similar constructs: A conceptual clarification. In *Proceedings of the 8th international Conference on Electronic Commerce: the New E-Commerce: innovations For Conquering Current Barriers, Obstacles and Limitations To Conducting Successful Business on the internet* (Fredericton, New Brunswick, Canada, August 13-16, 2006). ICEC '06, vol. 156. ACM, New York, NY, 235-243.

Gross, J. B. & Rosson, M. B. (2007). Looking for trouble: understanding end-user security management. In *Proceedings of the 2007 Symposium on Computer Human interaction For the Management of information Technology* (Cambridge, MA, March 30-31, 2007). CHIMIT '07. ACM, New York, NY, 10.

Hebert, A. J. (2005). Information Battleground. *Air Force Magazine, Journal of the Air Force Association*, 88(12). Retrieved August 30, 2007, from: http://www.afa.org/magazine/Dec2005/1205info.html

Hilton, J. L., Fein, S., & Miller, D. T. (1993). Suspicion and dispositional Inference. *Personality and Social Psychology Bulletin*, 19(5), 501-512.

Hollebeek, T. & Waltzman, R. (2004). The role of suspicion in model-based intrusion detection. In *Proceedings of the 2004 Workshop on New Security Paradigms* (Nova Scotia, Canada, September 20-23, 2004). NSPW '04. ACM, New York, NY, 87-94.

Horn, D. B. (2001). Is seeing believing?: Detecting deception in technologically mediated communication. In *CHI '01 Extended Abstracts on Human Factors in Computing Systems* (Seattle, Washington, March 31 - April 05, 2001). CHI '01. ACM, New York, NY. 297-298.

Hubbell, A. P., Mitchell, M. M., & Gee, J. C. (2001). The relative effects of timing suspicion and outcome involvement on biased message processing. *Communication Monographs*, 68(2), 115-132.

Hudson, B. (2004). Trust: Towards conceptual clarification. *Australian Journal of Political Science*, 39(1), 75-87.

Jones, G. R., & George, J. M. (1998). The experience and evolution of trust: Implications for cooperation and teamwork. *Academy of Management Review*, 23, 531-546.

Kee, H. W. & Knox, R. E. (1970). Conceptual and methodological considerations in the study of trust and suspicion. *Journal of Conflict Resolution*, 14(3), 357-366.

Kephart, B. (2004). In us we trust. *Science & Spirit* [Electronic version]. Retrieved November 14, 2007, from: http://www.science-spirit.org/article_detail.php?article_id=442

Korukonda, A. R. (2005). Personality, individual characteristics, and predisposition to technophobia: some answers, questions, and points to ponder about. *Information Sciences*, 170(2-4), 309-328.

Lee, K. M. & Nass, C. (2003). Designing social presence of social actors in human computer interaction. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, FL, April 05-10, 2003). CHI '03. ACM, New York, NY, 289-296.

Levine, T. R. & McCornack, S. A. (1991). The dark side of trust: Conceptualizing and measuring types of communicative suspicion. *Communication Quarterly*, 39(4), 325-340.

Lewicki, R. J., Tomlinson, E. C., Gillespie, N. (2006). Models of interpersonal trust development: Theoretical approaches, empirical evidence, and future directions. *Journal of Management*, 32(6), 991-1022.

Lewicki, R.J. & Stevenson, M. (1998). Trust development in negotiation: Proposed actions and a research agenda. *Journal of Business and Professional Ethics*, 16(1-3), 99-132.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces*, 63(4), 967-985.

Marchand, M. A. G. & Vonk, Roos (2005). The process of becoming suspicious of ulterior motives. *Social Cognition*, 23(3), 242-256.

McCornack, S. A. & Levine, T. R. (1990). When lovers become leery: The relationship between suspicion and accuracy in detecting deception. *Communication Monographs*, 57(3), 219-230.

McCornack, S. A., & Parks, M. R. (1986). Deception detection and relationship development: The other side of trust. In M. L. McLaughlin (Ed,). *Communication Yearbook 9*, Beverly Hills; Sage. (377-389).

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review*, 23(3), 473-490.

McKnight, D. H. & Kacmar, C. J. (2007). Factors and effects of information credibility. In *Proceedings of the Ninth international Conference on Electronic Commerce* (Minneapolis, MN, August 19-22, 2007). ICEC '07, vol. 258. ACM, New York, NY, 423-432.

Millar, M. G. & Millar, K. U. (1997). The effects of cognitive capacity and suspicion on truth bias. *Communication Research*, 24(5), 556-570.

Muir, B. M. (1987). Trust between humans and machines, and the design of decision aids. International Journal of Man-Machine Studies, 27(5-6), 527-539.

Murphy, L. L., Stanney K., & Hancock, P. A. (2003). The Effect of affect: a hedonomic evaluation of human computer interaction. In *Proceedings of the 47th Annual Meeting of the Human Factors and Ergonomics Society*, Denver, CO, 764-768.

Nass, C., Moon, Y., Fogg, B., Reeves, B., & Dryer, C. (1995). Can computer personalities be human personalities?. In *Conference Companion on Human Factors in Computing Systems* (Denver, Colorado, United States, May 07-11, 1995). I. Katz, R. Mack, and L. Marks, Eds. CHI '95. ACM, New York, NY, 228-229.

Nass, C., Steuer, J., & Tauber, E. R. (1994). Computers are social actors. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems: Celebrating interdependence* (Boston, MA, April 24-28, 1994). B. Adelson, S. Dumais, and J. Olson, Eds. CHI '94. ACM, New York, NY, 72-78.

Neumann, P. G. (1989). The computer-related risk of the year: Misplaced trust in computer systems. In *Proceedings of the Fourth Annual IEEE Computer Assurance Conference* (June 20-23, 1989), Gaithersburg, MD, 9-13.

Northcutt, N. & McCoy, D. (2004). Interactive Qualitative Analysis: A systems method for qualitative research. Thousand Oaks, CA: Sage.

Qin, T., Burgoon, J., & Nunamaker, J. F. (2004). An Exploratory Study on Promising Cues in Deception Detection and Application of Decision Tree. In *Proceedings of the Proceedings of the 37th Annual Hawaii International Conference on System Sciences (Hicss'04) - Track 1 - Volume 1* (January 05-08, 2004). HICSS. IEEE Computer Society, Washington, DC, 2.

Quattrone, G. A. (1982). Overattribution and unit formation: When behavior engulfs the person. *Journal of Personality and Social Psychology*, 42, 593-607

Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: a framework for research and design. *International Journal of Human-Computer Studies,* 62(3), 381-422.

Roberts, P. F. (2006) Future-proof your IT security, [Electronic Version]. *InfoWorld*. Retrieved March 13, 2007, from: http://www.infoworld.com/article/06/10/30/44FEsecfuture_1.html

Ross, L. (1977). The intuitive psychologist and his shortcomings: Distortions in the attribution process. In L. Berkowitz (Ed.) *Advances in experimental social psychology*. 10, 173-220. New York: Academic Press.

Rotter, J. (1967). A New Scale for the Measurement of Interpersonal Trust, *Journal of Personality*, 35, 651-665.

Rotter, J. B. (1971). Generalized expectancies for interpersonal trust. *American Psychologist*, 26(5), 443-452.

Rotter, J. B. (1980). Interpersonal trust, trustworthiness and gullibility," *American Psychologist*, 35(1), 1-7.

Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of Management Review*, 23(3), 393-404.

Rozanski, E. P. & Haake, A. R. (2003). The many facets of HCI. In *Proceedings of the 4th Conference on Information Technology Curriculum* (Lafayette, IN, October 16-18, 2003). CITC4 '03. ACM, New York, NY, 180-185.

Shechtman, N. & Horowitz, L. M. (2003). Media inequality in conversation: how people behave differently when interacting with computers and people. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Ft. Lauderdale, FL, April 05-10, 2003). CHI '03. ACM, New York, NY, 281-288.

Stiff, J. B., Kim, H. J. & Ramesh, C. N. (1992). Truth biases and aroused suspicion in relational deception. *Communication Research*, 19(3), 326-345.

Toris, C. & DePaulo, B. M. (1985). Effects of actual deception and suspiciousness of deception on interpersonal perceptions. *Journal of Personality and Social Psychology*, 47(5), 1063-1073.

Tschannen-Moran, M. & Hoy, W. K. (2000). A multidisciplinary analysis of the nature, meaning, and measurement of trust. *Review of Educational Research*, 70(4), 547-593.

Turner, J. M. (2006). *The Communications of Influence through Technology-Enabled Media*. PhD dissertation. University of Texas, Austin, TX (ADA462849).

Trope, Y. (1989). Levels of inference in dispositional judgment. *Social Cognition*, 7(3), 296-314.

Tversky A., & Kahneman D. (1974). Judgment under uncertainty: Heuristics and biases. *Science 185*, 1124–1134.

United States General Accounting Office [US GAO] (2004). *Knowledge of Software Suppliers Needed to Manage Risks*: *Report to Congressional Requesters on Defense Acquisitions*. GAO-04-678. Washington: GAO.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M. (1998). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review*, 23(3), 513-530.

Zuckerman, M., DePaulo, B. M., & Rosenthal, R. (1981). Verbal and nonverbal communication of deception. In L. Berkowitz (Ed.), *Advances in Experimental Social Psychology*, 14, 1-59). New York: Academic Press.

Zuckerman, M., Kernis, M. R., Driver, R., & Koestner, R. (1984). Segmentation of behavior: Effects of actual deception and expected deception. *Journal of Personality and Social Psychology*, 46(5), 1173–1182.

Vita

Captain Henry G. Paguirigan enlisted in the United States Air Force soon after graduating from Radford High School in Honolulu, Hawaii. As a prior-enlisted member, he has served on numerous assignments as an Electrical Systems Technician for Civil Engineering. During his enlistment, Captain Paguirigan completed his Bachelor of Science Degree in Occupational Education/Management, from Wayland Baptist University in San Antonio, Texas. After graduating from Officer Training School, his first assignment as a communications officer was with the 89th Communications Squadron, Andrews AFB, MD. His next assignment was with Detachment 4 AFOTEC as an analyst for a satellite test program. He entered the Graduate School of Systems and Engineering Management at The Air Force Institute of Technology on September 2006. Upon graduation, he will be assigned to PACAF, Hickam AFB, HI.

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

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

PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
27-03-2008	Master's Thesis	Aug 2007 - Mar 2008

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Suspicion Modeling in Support of Cyber-Influence Operations/Tactics	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Paguirigan, Henry, G., Captain, USAF	N/A
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way WPAFB OH 45433-7765	AFIT/GIR/ENV/08-M17
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
Intentionally left blank	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMTED

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Understanding the cognitive process of IT user suspicion may assist organizations in development of network protection plans, personnel training, and tools necessary to identify and mitigate nefarious intrusions of IT systems. Exploration of a conceptual common ground between pycho-social and technology-related concepts of suspicion are the heart of this investigation. The complexities involved in merging these perspectives led to the overall research question: What is the nature of user suspicion toward IT? The research problem/phenomenon was addressed via extensive literature review, and use of the Interactive Qualitative Analysis methodology. A focus group consisting of military IT professionals identified their representative system of the problem/phenomenon. Analysis of the system led to the development of a model of IT suspicion as a progenitor for future experimental constructs that measure or assess behavior as a result of cyber attacks.

15. SUBJECT TERMS

Suspicion, Trust, Information Technology, Human-Computer Interaction, Deception Detection

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Jason M. Turner, Maj, USAF
U	U	U	UU	124	19b. TELEPHONE NUMBER (Include area code) 937-255-3636 ext.7407 jason.turner@afit.edu

Standard Form 298 (Rev. 8/98)
Prescribed by ANSI Std. Z39.18