

Air Force Institute of Technology

AFIT Scholar

---

Theses and Dissertations

Student Graduate Works


---

3-2020

## Recognizing Potential Cyberspace Warriors through the Use of Suspicion Propensity Index

Meghan G. Strang

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

 Part of the [Operations Research, Systems Engineering and Industrial Engineering Commons](#), and the [Training and Development Commons](#)

---

### Recommended Citation

Strang, Meghan G., "Recognizing Potential Cyberspace Warriors through the Use of Suspicion Propensity Index" (2020). *Theses and Dissertations*. 3257.  
<https://scholar.afit.edu/etd/3257>

This Thesis is brought to you for free and open access by the Student Graduate Works at AFIT Scholar. It has been accepted for inclusion in Theses and Dissertations by an authorized administrator of AFIT Scholar. For more information, please contact [richard.mansfield@afit.edu](mailto:richard.mansfield@afit.edu).



**RECOGNIZING POTENTIAL CYBERSPACE WARRIORS THROUGH THE  
USE OF SUSPICION PROPENSITY INDEX**

THESIS

Meghan G. Strang, Second Lieutenant, USAF

AFIT-ENV-MS-20-M-244

**DEPARTMENT OF THE AIR FORCE  
AIR UNIVERSITY**

**AIR FORCE INSTITUTE OF TECHNOLOGY**

**Wright-Patterson Air Force Base, Ohio**

**DISTRIBUTION STATEMENT A.  
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. This material is declared a work of the U.S. Government and is not subject to copyright protection in the United States.

AFIT-ENV-MS-20-M-244

RECOGNIZING POTENTIAL CYBERSPACE WARRIORS THROUGH THE USE OF  
SUSPICION PROPENSITY INDEX

THESIS

Presented to the Faculty

Department of Systems Engineering and 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 Engineering Management

Meghan G. Strang, BS

Second Lieutenant, USAF

March 2020

**DISTRIBUTION STATEMENT A.**  
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

AFIT-ENV-MS-20-M-244

RECOGNIZING POTENTIAL CYBERSPACE WARRIORS THROUGH THE USE OF  
SUSPICION PROPENSITY INDEX

Meghan G. Strang, BS

Second Lieutenant, USAF

Committee Membership:

Michael E. Miller, PhD  
Chair

John J. Elshaw, PhD  
Member

Alfred E. Thal Jr., PhD  
Member

## Abstract

The Air Force currently suffers from excessively high attrition rates in the cyberspace career. The field is currently aiming to develop an entrance examination for the career, striving to improve personnel selection and decrease these high attrition rates. The attribute of suspicion is a key focus of the preliminary examination development, theorizing that it is a potential indicator present among competent cyber operators. This research makes use of the Suspicion Propensity Index (SPI), a reliable measure of one's tendency to be suspicious, along with the highly cited Mayer's trust questionnaire in order to compare the attributes that appear in successful cyberspace individuals compared to those with no cyber experience. These measures are analyzed in comparison to a cyber mission performance questionnaire, adapted to assess each participant's cyberspace capabilities. The three aforementioned questionnaires were distributed to two distinct populations: a group of experienced cyber operators averaging 22.8 years in the career field and a group of Airmen from various career fields with no prior cyber experience.

The research yields evidence that suspicion levels are significantly correlated to cyber mission performance scores among both the cyber and non-cyber populations, with cyber operators demonstrating higher overall levels of suspicion than those of non-cyber operators. Years of experience displays a more prominent effect on the suspicion levels of cyber personnel, with the non-cyber sample population displaying more constant levels of suspicion despite time in the Air Force. This evidence suggests that cyber operators gain suspicion over time in comparison to their non-cyber counterparts. The trust questionnaire scores were significantly correlated to SPI scores. However, results of the trust questionnaire do not appear to provide a prediction of cyber mission performance.

## **Acknowledgments**

I would like to express my sincerest gratification to my research advisor, Dr. Miller. His feedback and words of encouragement provided me with the necessary toolset to conduct this research. The insight and perspective was greatly appreciated. I would also like to thank Dr. Elshaw for always being readily available to guide me through the data analysis process, and for providing new ideas whenever needed. Lastly, I would like to thank Dr. Bobko for being a constant motivation and supporting figure throughout this research. His knowledge and positivity granted me with the enthusiasm necessary to complete this thesis.

Meghan G. Strang

## Table of Contents

	Page
Abstract.....	iv
Acknowledgements.....	v
Table of Contents.....	vi
List of Figures.....	viii
List of Tables.....	ix
I. Introduction.....	
1.1 General Issue.....	1
1.2 Problem Statement.....	6
1.3 Research Objectives.....	7
1.4 Research Questions.....	9
1.5 Research Hypotheses.....	9
1.6 Research Focus/Scope.....	10
1.7 Methodology Overview.....	10
1.8 Assumptions/Limitations.....	11
1.9 Implications.....	12
II. Literature Review.....	
2.1 Literature-Based Construct of Suspicion.....	14
2.2 Trust and its Role in Suspicion.....	20
2.3 Cyber Warrior Development and Research.....	22
2.4 Summary.....	27
III. Methodology.....	
3.1 Chapter Overview.....	28
3.2 Participants.....	28
3.3 Measures.....	29
3.4 Procedure.....	32
3.5 Analysis Overview.....	33
3.6 Summary.....	33
IV. Analysis and Results.....	



4.1 Chapter Overview.....	34
4.2 Performance Measurement.....	34
4.3 Descriptive Statistics and Correlations.....	36
4.4 Suspicion and Performance .....	38
4.5 Suspicion Among Cyber vs Non-Cyber Personnel .....	40
4.6 Effects of Years Experience .....	41
4.7 Trust and Performance .....	44
4.8 Summary .....	45
V. Conclusions and Recommendations .....	47
5.1 Chapter Overview.....	48
5.2 Evaluation of Research Questions.....	48
5.3 Significance of Research .....	50
5.4 Recommendations for Future Research .....	52
5.5 Summary .....	53
Appendix A: Demographics Questionnaire .....	54
Appendix B: Suspicion Propensity Index .....	55
Appendix C: Personality Questionnaire.....	61
Appendix D: Mission Scenario Questionnaire .....	62
Bibliography .....	64

## List of Figures

	Page
Figure 1. Causal Loop Diagram for considerations for the selection process of individuals into the cyber career field.....	4
Figure 2. The 3 stages that encompass a suspicious state.....	16
Figure 3. Influencing factors on situational trust.....	18
Figure 4. Influencing factors on dispositional trust.....	19
Figure 5. Cyber Mission Force Training Phase Model.....	23
Figure 6. Distribution of performance scores among cyber and non-cyber personnel....	38
Figure 7. Distribution of SPI scores among cyber and non-cyber personnel. ....	42
Figure 8. Two-way interaction between career and years in service on suspicion scores. .....	44

## List of Tables

	Page
Table 1. Measurements Questionnaires .....	30
Table 2. Performance score mean comparison among non-cyber (0) and cyber (1) populations .....	<b>Error! Bookmark not defined.</b> 34
Table 3. Descriptive Statistics.....	36
Table 4. Correlations for all variables.....	37
Table 5. SPI as predictor for performance score.....	39
Table 6. Cyber and non-cyber SPI scores .....	41
Table 7. Interaction between years in service and career on suspicion scores .....	43
Table 8. Trust measurements as a predictor for performance.....	45
Table 9. Predictive capability of the combined effect of trust and suspicion. ....	46

# **RECOGNIZING POTENTIAL CYBERSPACE WARRIORS THROUGH THE USE OF SUSPICION PROPENSITY INDEX**

## **I. Introduction**

### **1.1 General Issue**

As war fighting in the cyber domain rapidly evolves, the Air Force must be equipped with the finest airmen capable of innovating technology, techniques, tactics, and procedures to continually improve the United States' offensive and defensive capabilities on a global level. Innovation in the cyber domain is critical to fulfill the Air Force's mission and to pursue excellence in the air, space, and cyberspace domains. Despite the Air Force mission's emphasis placed in the cyberspace domain, this area lacks the same personnel selection, training, and structural foundation as the companion domains of air and space.

To maintain dominance in the air, the Air Force carefully selects well-equipped pilot candidates from Reserve Officer Training Corps (ROTC) detachments, Officer Training School, and the country's service academies. Candidate Pilots are held to strict standards and must meet multiple qualifications before being considered eligible for the career field. For example, they must have a minimum education of a bachelor's degree with a grade point average greater than 2.5 and obtain certain scores on the pilot portion and pilot-navigator portion of the Air Force Officer Qualifying Test (U.S. Air Force). Pilot training is rigorous, multiple years long, and therefore expensive to conduct for each pilot trainee. Yet this in-depth training is necessary to ensure that the United States is equipped with the finest airmen to conduct specific operations. Select individuals within this career field are engaged to refine future techniques, tactics and procedures, as well as provide guidance to the acquisition community to evolve technical capabilities.

Airmen selected for careers in the space field are also carefully selected, as the field requires a basic background knowledge of space warning and control systems. Space Operations Officers are required to have the minimum education of a bachelor's degree in a science, technology, engineering, or math (STEM) discipline, while enlisted Space Operators are required to have at least 15 college credits in a STEM field along with meeting certain scores on the electrical component of the Armed Services Vocational Aptitude Battery (ASVAB) test (U.S. Air Force). In addition to the background requirements for knowledge in the field, Undergraduate Space Training is a rigorous six-month program and is only the foundation for additional system-specific training that must be completed.

While the Air Force strives to dominate in air, space, and cyberspace, there is a clear dissonance between the qualifications for the cyber field in comparison to the other two domains. Dissimilar to the air and space components, the cyber component lacks the strenuous prerequisite demands and does not necessitate any rigid credentials before entering the field. The cyber career field also suffers from extremely high attrition rates during training activities, highlighting it as one of the Air Force's top manning priorities in 2017, 2018, and 2019 (Losey, 2018). These attrition rates have brought attention to the field in hopes of meeting the increasing quotas for cyber airmen and their likelihood to remain in the field.

One potential option for the Air Force is to enhance the selection criteria for cyberspace airmen, consequently boosting the knowledge that individuals must obtain prior to entering the field. However, individuals with prerequisite computer science skills are in high demand within both the civilian and government realms. Computer engineering holds one of the highest paying starting salaries for students graduating with a college degree (Somers & Moody, 2019). The financial incentives associated with careers in this field may be one of the reasons that the

number of computer science bachelor's degrees has risen by 74% since 2009 (Hambrusch, 2017). While the number of graduates who are competent in the realm of computer science and computer engineering is growing, so is the industry's need for individuals with this skillset. This demand makes it critical for the Air Force to carefully balance the Human Systems Integration domains of personnel, manpower, and training when considering which airmen are best fit for the cyber career field.

As cyber selection currently operates, a large number of commissioned and enlisted Airmen are assigned to the field to cushion the high attrition rate. This reduces the average workforce cost as it relieves the Air Force from paying above market salaries to entice a smaller number of more experienced, highly educated, cyber personnel. However, by accepting Airmen who require greater amounts of training to prepare them to be successful operators in the cyber field and make them mission-ready, training costs are increased. If selection criteria was more stringent for the field as a whole, fewer individuals should wash out of training, it may be possible to enhance the quality of the training, and it is possible that a lesser number of highly capable individuals, as opposed to larger groups of less capable individuals, would be needed to execute the Air Force's cyber needs. Figure 1 is a causal loop diagram displaying the balance between the different considerations in respect to the cyber field. To choose the optimal quantity and quality of individuals in the career field, many interconnected factors must be taken into consideration. Manpower is made possible by material support and the cost of retaining the number of individuals in the field. It in turn affects the cost of personnel, which forms a cyclical pattern by affecting retention costs. Experience in the cyber field is another consideration that plays a role in the cost of personnel, along with selection criteria which also affects the cost and quality of training.

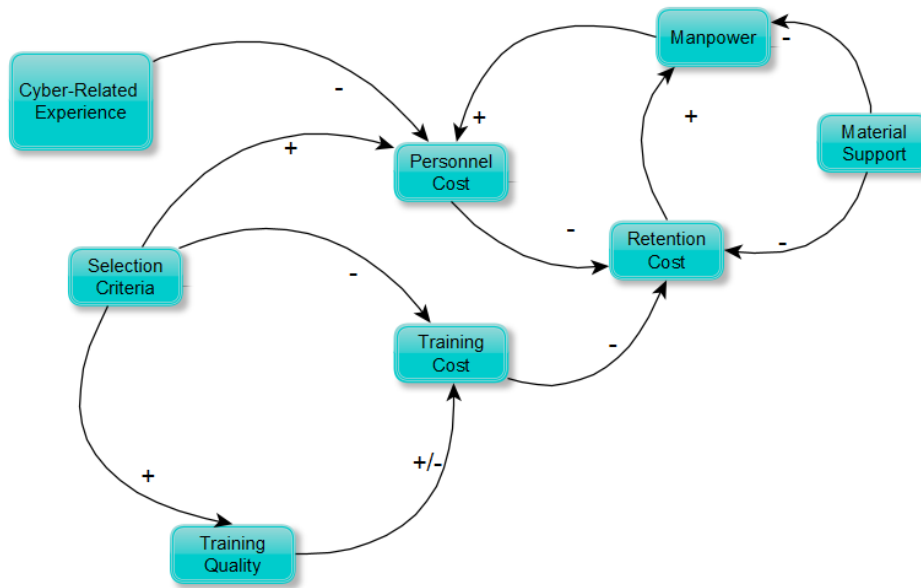


Figure 1. Causal Loop Diagram for considerations for the selection process of individuals into the cyber career field.

To properly select individuals with a predisposition for success as cyber operators, one option is the development of an entrance examination for the career field. This examination could be extremely beneficial to filter out individuals who lack the foundational attributes that are needed within the field, along with identifying those who are prone to success.

The use of an entrance examination for specific career fields in the Air Force is a practice that has been successfully instilled throughout many career fields. The Air Force Officer Qualifying Test (AFOQT) is used in combination with the Pilot Candidate Selection Method (PCSM) to identify qualified candidates for flying career fields such as pilot, air battle management (ABM), and combat systems officer (CSO). The AFOQT is particularly beneficial for officers seeking to go into the rated career field with no prior flying experience. In a 2013 study, of 139 Undergraduate Remotely Piloted Aircraft (RPA) Training students who took the PCSM and AFOQT prior to beginning training, the scores exemplified good predictive validity

(AFOQT  $r = 0.378$ , PCSM  $r = 0.48$ ) for determining completion of the undergraduate training (Carretta, 2013). Thus, individuals who were successful on this initial examination were significantly more likely to successfully complete training than individuals who were not successful on this examination. This study portrays the importance of selecting individuals with little to no experience based on their propensity for success in the career field. To implement a similar examination for the cyber career field, testing categories should aim to screen for cyber-propensity as opposed to exclusively testing for current cyber knowledge.

In addition to rated career fields, certain jobs requiring fluency in foreign language use quantitative measures to gauge an individual's fitness for these career fields. The Defense Language Proficiency Test (DLPT) is used for individuals who are already fluent in a foreign language which is needed for current military operations. As the test is currently scored, a person's language proficiency is measured on a scale of zero to three with three being the highest. However, a newer version of the DLPT is being developed that will include a scale from zero to five. Another proficiency exam includes the Defense Language Aptitude Battery (DLAB), which measures one's aptitude for learning a specific language. This is more commonly used for individuals who are not currently fluent in a language that is needed by the Department of Defense (DOD), but who are seeking a job that requires this skill. To develop a DLAB similar entrance exam for the cyber career field, the Air Force must first understand exactly what traits and characteristics make an individual more adept for cyber operations.

This requirement has been recognized by the Air Force and has resulted in the generation of a need for additional exploration. This research is being conducted in response to the topic "Recognizing Potential Cyberspace Warriors" within the Air University Prioritized Research



Topics within the Cyber category. The research discussed in this thesis attempts to help foster an entrance examination, which is claimed to be under preliminary development through the addition of a questionnaire focused on understanding the propensity of a person to be suspicious. Cyber operators are required to install and support cyber systems, along with ensuring their proper operation and protection from outside intrusion. The preliminary belief that suspicion is a helpful attribute within the cyber career field stems from the tendencies of suspicious personnel. Suspicion allows individuals to recognize unusual items or actions in specific situations, while a natural tendency towards curiosity allows suspicious individuals to elicit information and surveil for potentially threatening actions. If an individual is naturally inclined to be suspicious and prone to act upon these tendencies, they may be able to bolster cyber capabilities by maintaining safe and secure operations. The overall objective of this research is to assist in the Air Force's development of the entrance examination. This research aims to reveal insightful information regarding how suspicion correlates with successful operators in the cyber field.

## **1.2 Problem Statement**

The Air Force cyber career field lacks a field-specific entrance examination for its officer and enlisted airmen. This lack of a screening process is partially responsible for the field's suffering from high attrition rates and low retention among its personnel. If the career field could determine specific attributes that are correlated with success as a cyberspace warrior, it may help reduce washout rates and develop a more effective cyberspace domain in the Air Force as a whole. The long-term objective of the current work is to create a screening tool, aiming to reduce washout rates and increase retention in the cyberspace domain, thus saving manpower and training dollars for the United States Air Force.

### 1.3 Research Objectives

In consideration of the cyber environment and the actions which take place within the cyber domain, both human performance and hardware/software performance compromise the overall system performance. While a vast amount of research is constantly being conducted to improve technological capabilities, research is sparse regarding which attributes affect the human operator while conducting cyber operations. This research will investigate suspicion, aiming to identify its contribution to operator performance in the cyber field. It will also investigate trust as a potential inverse characteristic of suspicion.

As it is currently accepted, suspicion is a state attribute that is affected by individual differences of the perceiver. Recent studies have revealed that for a person to enter a state of suspicion, the individual is first aroused by a specific trigger within her or his environment. This cue is then interpreted by the individual in regard to their specific personality traits and propensity to be suspicious. If the individual is sufficiently aroused, he or she will enter a suspicious state (Bobko et al., 2014). It has been recently concluded that at different situational levels, individual personality differences are responsible for either inhibiting or catalyzing this state of suspicion (Khazon, 2016).

A suspicious state is one that produces uncertain feelings in regard to the individual's environment, a feeling of malicious intent towards the trigger that is responsible for the suspicious state, along with cognitive activity such as indications of stress, perceived increase of cognitive load, and heightened emotional arousal (Khazon, 2016). For example, a cynical individual will interpret the suspicion of a situation differently than that of a person who holds great faith in humanity.

Another potential individual trait that may affect suspicion is the predisposition for trust and/or distrust. As suspicion relies partially on one's uncertainty in a situation, a predisposition for trust has the potential to increase levels of certainty within a specific context. Contrarily, distrust may act as a catalyzing factor for an increase in suspicion (Mayer & Mussweiler, 2011).

This research posits that one's propensity for the attribute of suspicion will yield a relevant correlation with mission performance in the cyber career field. State suspicion propensity is defined as "a person's simultaneous state of cognitive activity, uncertainty, and perceived malintent about underlying information that is being electronically generated, collated, sent, analyzed, or implemented by an external agent" (Bobko, Barelka, Hershfield, 2014). This research will aim to measure the attributes of an individual's propensity for suspicion, perception of malintent, uncertainty of information, and the engagement in cognitive activity associated with generating meanings for possible information in relation to his or her experience and expertise in the cyber career field. This research will also aim to determine whether individuals who have been successful in the cyber career field will exhibit a greater propensity for the attribute of suspicion than members of other career fields in the Department of Defense.

As the characteristic of suspicion is proving to be a prevalent area of focus in the field of cyberspace operations, an objective of this study is to investigate the means in which an enhanced understanding of how suspicion's role amongst cyber operators could assist in the development of an effective screening tool for entrance to the career field. Through a number of surveys and questionnaires, this research aims to explore how the information collected on current members of the cyber career compares to the same information gathered from their non-cyber counterparts with the aim of providing insight into whether the Air Force and military at large should explore

measures of the characteristic of suspicion and trust to assist in their selection process for future cyber warriors.

#### **1.4 Research Questions**

The following research questions (RQ) will be investigated throughout this study:

- 1.4.1 (RQ-1): Is an individual's level of suspicion correlated to her or his success within the cyberspace career field?
- 1.4.2 (RQ-2): Do current Air Force cyber operators differ in their levels of suspicion when compared to members of other career fields?
- 1.4.3 (RQ-3): Does an Airman's years of experience in their field correlate to significant differences in levels of suspicion?
- 1.4.4 (RQ-4): Does an Airman's propensity to trust correlate with both her or his levels of suspicion and success within the cyberspace career field?

#### **1.5 Research Hypotheses**

The following research hypotheses (RH) were developed in relation to the research questions:

- 1.5.1 (RH-1): An individual's scores on the SPI and the Mission Scenario questionnaire will yield a positively correlated relationship. Those who score high on the SPI will also do well on the Mission Scenario Questionnaire, and vice versa.
- 1.5.2 (RH-2): Suspicion levels and career field are not independent, thus cyber operators will yield higher SPI scores in comparison to members of other career fields.

- 1.5.3 (RH-3): Years of experience will have a positive correlation to an individual's SPI score. This correlation will be stronger within the cyber career field than that of other career fields.
- 1.5.4 (RH-4): Trust questionnaire scores will yield a negative correlation with both an individual's SPI score and her or his Mission Scenario questionnaire score.

## **1.6 Research Focus/Scope**

Within the realm of this study, cyber operators were expected to exhibit higher levels of suspicion than airmen of other career fields, as well as exhibit increased levels of suspicion with increased experience. Trust was also expected to display a negative relationship with both suspicion and cyber performance. These hypotheses have the potential to significantly impact the selection process for operators entering the cyber career field. The identification of suspicion and trust as traits potentially correlated to the predisposition for success in cyber operations has the capacity to assist the Air Force in screening individuals entering the field. This study also expected a general increase in suspicion levels as individuals gain more experience, with the rate of increase being higher in cyber operators. This may indicate that suspicion is a trainable attribute and that it can be developed in individuals over time. These increases would yield useful results for the Air Force throughout their cyber personnel selection process, as they would allow the measurement of suspicion to be adjusted regarding a person's age and background.

## **1.7 Methodology Overview**

Multiple measurement methods provided a basis for data collection within this thesis to include a demographics questionnaire, a Suspicion Propensity Index, trust assessment, and mission scenario questionnaire. The demographics questionnaire was administered to gather pre-survey

information about the participants. Next, an eleven-item Suspicion Propensity Index (Bobko et al., n.d.) was given to measure the components of each individual's level of suspicion, including that of cyber operators and non-cyber operators. Trust was assessed through an eight-item survey designed to measure both trust and distrust (Mayer, Davis & Schoorman, 1995). Performance at various cyber operations was measured through a six-item survey, referred to as the Mission Performance Questionnaire, in which different scenarios were presented to the participants and they were instructed to choose the best response to each case. A total of 122 individuals participated in this research, including 57 from the cyber career field and 65 from career fields other than cyber. Data was analyzed using multiple techniques to include simple linear regression, T-tests, correlation tables, and multiple linear regression.

### **1.8 Assumptions/Limitations**

The current research is not intended to develop an all-encompassing personnel selection tool, but rather to consider whether suspicion as a trait attribute may be one of multiple useful criteria useful in the development of such a tool. It is recognized that other influences, such as an individual's preemptive interest in cyberspace operations, aptitude in the computer science realm, greater interest in other career fields, etc. may be more important than suspicion when selecting individuals for participation in the cyberspace career field.

A potential limitation of this study is not having access to the individuals who are currently undergoing cyber training, as a way to measure preliminary suspicion and success throughout the preliminary training courses for the career field. Additional information that would be helpful but was not available is access to the individuals who did not successfully complete cyber training, including students who have failed the preliminary courses or withdrew from the career field for lack of the necessary skills to perform the necessary operations within the field. These individuals

could provide insight into personality types and suspicion propensity for unsuccessful career field candidates. However, due to the Privacy Act of 1974, the personal information for these individuals is protected which currently limits our ability to track individuals through the training process.

An additional limitation of this study arises from the sample of individuals participating in the Continuing Education Cyber courses at Wright-Patterson Air Force Base. It is a possibility that these individuals are not representative of the career field at large, resulting in a sampling bias. Due to the voluntary nature of the survey, it is also possible that only certain types of individuals participated in the study. This possibility also holds true for the non-cyber participants, as the surveys were also administered on a voluntary basis.

## **1.9 Implications**

If this research helps in the assessment of attributions correlated with successful airmen as cyberspace operators, it has the potential to reduce the cost and effort spent to train ill-equipped airmen who wish to enter the career field. With the current lack of a screening examination for the career field, many airmen are being assigned to cyber even though they may not have the knowledge or propensity for success in the current training program or the field. With the help of the SPI and other research on what makes a cyberspace airman effective, the Air Force should be able to select men and women who are more predisposed to success. This will decrease the chance that these men and women will wash-out of the training program, allowing these individuals to flourish in other fields. It will also allow for more focus and higher quality training for the individuals who do participate in the field's training program, leading to more knowledgeable and informed cyberspace airmen. This has great potential to eventually enhance the innovative techniques and improve our success against the nation's enemies. Lower washout rates amongst cyber training will also yield great savings in both time and money for the DoD as a whole.

In the human factors and psychology academic fields of study, this research could provide extremely insightful information on an important topic that currently has received limited research. The element of suspicion is an important topic as it plays a role in everyday life at both the individual and organizational level. By further exploring this topic, many opportunities could be created to provide insight into how humans interact with one another and with machines. Insight on suspicion has the potential to both explain and expand upon already existing theories in psychology, sociology, and other social sciences. Having such insights can improve organizational behavior through an understanding of suspicion, along with how these suspicion levels may be influenced under certain circumstances.



## II. Literature Review

### 2.1 Literature-Based Construct of Suspicion

The topic of suspicion is one that is relevant in many fields and its use in systems involving human-automation teams is likely to increase with growing dependence on automated systems in today's society. Although little investigation has been conducted in the past regarding the causes of suspicion and its effects on human interactions, scientists have recently attempted to uncover what suspicion really means and how it develops as a trait.

In the existing literature, suspicion has been studied as a relevant domain in social psychology, management and communication, marketing, and human factors psychology (Khazon, 2016). In social psychology, suspicion is defined as “a dynamic state in which the individual actively entertains multiple, plausibly rival hypotheses about the motive or genuineness of a person's behavior” (Fein, 1996). In communications and management literature, it is defined as “the degree to which a person is uncertain about the honesty of some specific communication content thereby stimulating a construal of motives in an effort to assess potential deceptive intent” (Kim & Levine, 2011). While different fields view suspicion through vastly different lenses, the literature has many common themes while describing the attribute that must be discussed.

**2.1.1 Uncertainty.** First, suspicion stems from a sense of uncertainty. Uncertainty occurs when an operator does not have enough information regarding a target to foresee a future action. The presence of uncertainty has been commonly studied in negotiation strategies, persuasive tactics, and in managerial positions. A common theme of these studies involves suspension of judgement and delayed decisions due to doubt one has when interacting with another entity

(Hilton, Fein, & Miller, 1993). Uncertainty alone is only one important facet of suspicion and does not act independently in the characteristic. For example, a person can be uncertain about a technology or software due to lack of training, but this does not mean that they are necessarily suspicious of its functionality (Bobko et al., 2014).

**2.1.2 Malicious Intent.** Malicious intent, often abbreviated to “malintent,” implies some form of dishonesty or attempt at manipulation by an outside source to harm or degrade the performance of the operator. An operator experiences malicious intent when they question one’s motives and perception of interference with their own goals, or cause harm in some other way (Khazon, 2016). The literature indicates that malicious intent acts in conjunction with uncertainty when an operator perceives the potential outcome of the uncertain action to have negative consequences. While it is possible for intent to be cast in a positive light, such as entrepreneurs taking risks in business ventures, the context of this study focuses on the negative instances that are associated with suspicion (Bobko et al., 2014).

**2.1.3 Cognitive Activity.** The final element of the accepted suspicion definition is cognitive activity. Cognitive activity refers to the mental processing that is required to predict incentives and future outcomes when dealing with the target. Several literatures have shown that a state of suspicion is correlated with higher activation levels when processing information, along with higher levels of engagement and thought processes (Kim & Levine, 2011).

In an attempt to synthesize these commonalities into one generally accepted definition, Bobko et al. (2014) conducted a study on suspicion in the Information Technology field and defined state suspicion as “a person’s simultaneous state of cognitive activity, uncertainty, and perceived malintent about underlying information that is being electronically generated, collated,

sent, or implemented by an external agent.” Using the vast amount of research available regarding trust and distrust through several domains, Bobko et al. (2014) attempted to relate suspicion to these characteristics and incorporated them into the introduction of a three-stage model, describing suspicion as a dynamic process. The model attempts to discuss how a person enters a suspicious state and then predict the immediate outcomes of this suspicion. A graphical depiction of the model is shown in Figure 2, followed by an in-depth description of each stage.

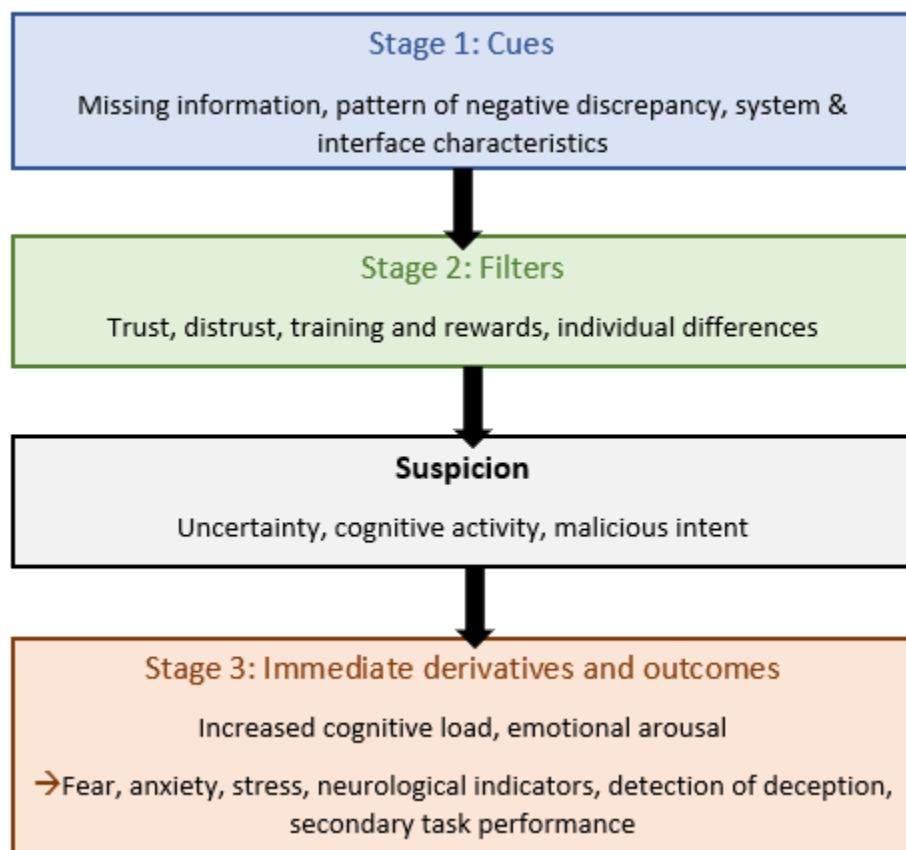


Figure 2. The 3 stages that encompass a suspicious state, adapted from Bobko et al., (2014).

**Stage I.** Stage I of Bobko’s three-stage model involves the perception and interpretation of environmental cues. Cues result in increased levels for uncertainty and malintent through a violation of the actor’s expectation from a target. The exposure to this violation results in a

trigger of state suspicion (Bobko et al., 2014). Environmental cues can have many patterns. These include the following:

*Missing information.* It has been shown that humans are wired to trust others in a community after they have opened up about personal life and revealed private information (Ridings, Gefen, & Arinze, 2000). Past research has also shown that when subjects perceive that policies are missing information, they are more likely to suspect that hidden motives are involved in the policy (Ebenbach & Moore, 2000). When information is absent as opposed to present, people are more likely to perceive the situation as suspicious.

*Patterns of negative discrepancy.* When users experience a dissonance between their expectations of system behavior and the behavior that is actually witnessed, state level suspicion is more likely to be cued (Bobko et al., 2014). Additionally, as subjects observe failures across a system, they are less likely to perceive the software as reliable. In the event that the operator views the system as undependable, they will be less likely to trust the system.

*System interface characteristics.* Usability characteristics such as video quality and response time have been found to correlate with increased levels of user trust (Lee & See, 2004). Situational trust, one of the three layers that comprise an individual's trust in automated systems, is described as being dependent upon specific content of an interaction between a user and a specific system (Hoff & Bashir, 2015). The factors depicted in Figure 3 are those that impact the development of trust and behavior within a particular situation.

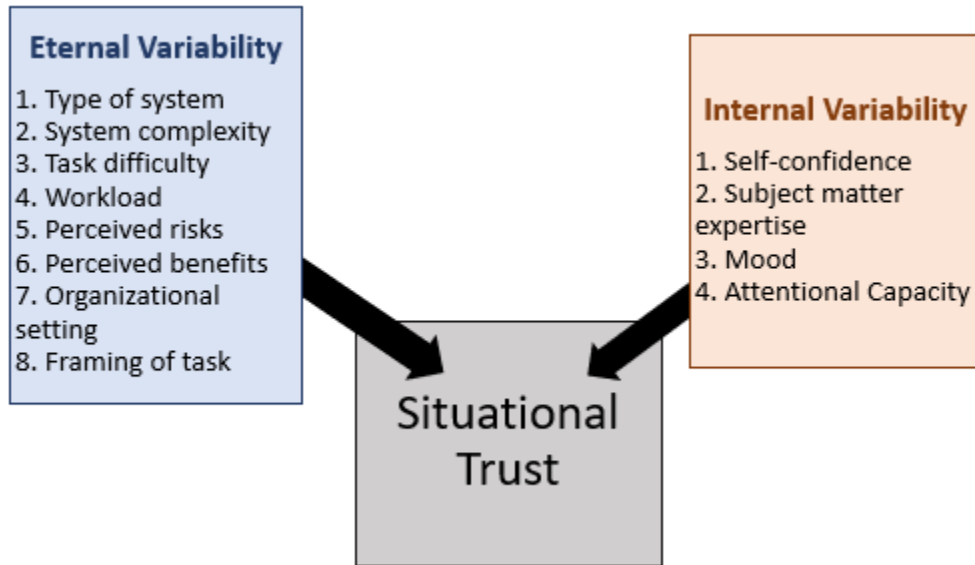


Figure 3. Influencing factors on situational trust, adapted from Hoff and Bashir (2015).

These factors directly influence one's interaction with a system and trust levels. When an individual is uncertain about these factors, suspicion is likely to be impacted.

**Stage II.** Stage II of the suspicion process model is the filtering stage. During this stage, the interpretation of environmental cues is influenced by an individual's characteristics. This includes one's prior life experiences, willingness to rely upon automated systems, and cognitive resources (Bobko et al., 2014). One's interpretation of environmental cues is also dependent upon trust propensity, also described as dispositional trust. Dispositional trust is trust that is independent of the context of a situation or the environment in which an interaction occurs. Instead, it is built upon individual characteristics that have been formed over a person's life through experience and biological influences. The factors that impact dispositional trust are shown in Figure 4 (Hoff & Bashir, 2015).

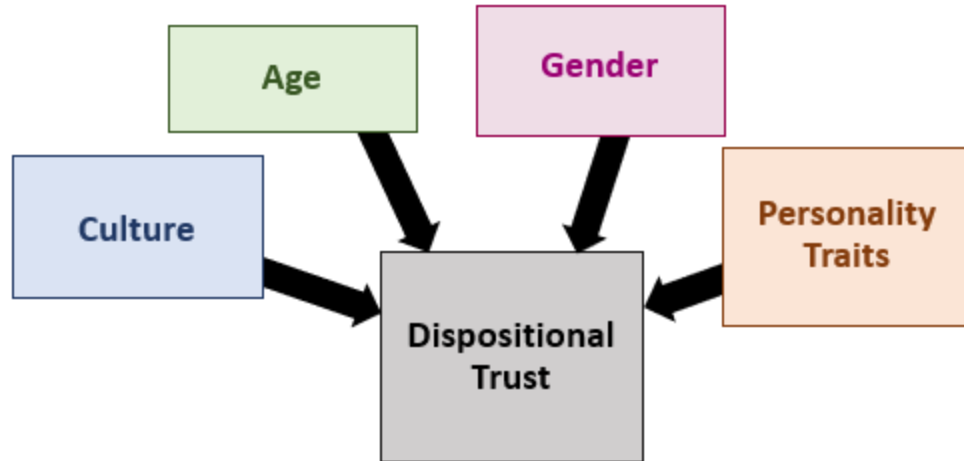


Figure 4. Influencing factors on dispositional trust, adapted from Hoff and Bashir (2015).

**Stage III.** The final stage of the suspicion process model is the formation and application of immediate outcomes. Based on the environmental cues and the different ways that individuals filter these cues in steps I and II, an immediate response is formed. If suspicious, a person will analyze the information collected and attempt to predict the next likely event that will occur given their response. This attempt to reduce uncertainty in the situation is thought to be both arousing and cognitively demanding (Khazon, 2016).

Bobko's et al. (2014) development of the process of suspicion is an initial leap in the direction of describing the process humans undergo during the arousal of suspicion. However, it only addresses state-suspicion and does not reveal the causes and consequences of an individual becoming suspicious over sustained periods of time. Several studies have shown that humans have limited mental resources and when participating in mentally stimulating activity, the activities associated with suspicion pull from the same group of resources. Execution of this process results in the depletion of mental resources and an overall decrease in performance for effortful cognitive activities. This includes a decrease in levels of vigilance (Smit, Eling, &

Coenen, 2004). As described by Bobko et al. (2014), state-suspicion is both mentally stimulating and demanding. These findings would suggest that a prolonged suspicious state would further diminish cognitive resources and cause fatigue that prevents the process from being sustained over time.

## **2.2 Trust and its Role in Suspicion**

Dictionary definitions of trust often include the description of “reliability,” “honesty,” and “assured anticipation.” In academia, one of the most commonly accepted definitions of trust is the “willingness of a party to be vulnerable to the actions of another party based on the expectations that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”, (Mayer, Davis, & Schoorman, 1995). Other definitions in research add to this definition, including a willingness to depend on others and the expectation of certain outcomes (Khazon, 2016). The notions of anticipation, expectation, and predictability are what link trust to suspicion in its definition. As described by Bobko et al. (2014), when an individual recognizes negative discrepancies and missing information from a situation, the result will be characterized by an increased rate of information searching, greater processing of available information, and the formation of plausible hypotheses for the observed behavior. The process includes actions designed to assist the formation of an expected outcome, thus increasing the state-like presence of trust and decreasing the suspicion in a situation.

It must be considered that when an individual has had no prior experience with an individual or cyber environment, he or she does not yet have any credible or meaningful information regarding that actor (Bigley and Pearce, 1998). As with most decision-making processes, one forms ideas based upon mental models and a set of rules that assist in the

development of opinions and beliefs (Falcone, Rino, et al., 2001). Interpretation rules allow individuals to categorize trust dilemmas and decide which evidence to search for in the assessment of another actor's trustworthiness. Action-based rules assist in deciding how to engage in response to certain interpretations. Initial trust is also believed to be based upon two interconnected components including one's willingness to depend and make themselves vulnerable, referred to as trusting intentions, and one's perceptions of the other actor's competence and integrity, referred to as trusting beliefs (McKnight, Choudhury, Kacmar, 2002). Each of the aforementioned processes and rules are applied to seek the common goal of gaining information which is useful in increasing the certainty in a situation, thus impacting suspicion.

While prevalent theories posit that trust and suspicion have an interdependent relationship, some theories hold that trust, distrust, and suspicion are separate entities (Lyons, 2011). These discrepant explanations of trust are distinguished from suspicion in their lack of presence of uncertainty. They claim that suspicion involves some ambiguity regarding a target's motives or intentions, while trust and distrust are characterized by confident feelings that a target will behave in a certain manner. A state of suspicion has also been described as "the occurrence of an event if the disconfirmation of the expectation of the event's occurrence is preferred to its conformation and if the expectation of its occurrence leads to behavior which is intended to reduce its negative motivational consequences" (Deutsch, 1958). In this viewpoint, trust is also described as the expectation of an occurring event which is perceived to have negative consequences if the expectation is not confirmed. These definitions separate trust and suspicion through the knowledge of a particular event, with suspicion being characterized by a lack of certainty in its occurrence and trust being the state that is achieved once sufficient certainty is achieved.



### **2.3 Cyber Warrior Development and Research**

It is no secret that the scope of the cyber career field and its capabilities are expanding within the United States Air Force and the military at large, as well as practically within all other government and many commercial enterprises. As the need for cyber defense and the capabilities of cyber increases, the need for capable personnel continues to expand. This growth includes large numbers of individuals with education in computer science and computer engineering, further depleting the available pool of individuals with this educational background. As such individuals within these disciplines are among the most sought after, resulting in more than one million unfilled computer science jobs in the United States in 2019 (Full Scale, 2019).

To compensate for the lack of academically trained individuals across the Air Force and other branches, the DoD has instituted a four-phase model in an attempt to rapidly train and

maintain a mission capable cyber mission force (CMF). The model is shown in Figure 5 (GAO, 2019).

	Phase one Basic individual training	Phase two Individual foundation training	Phase three Collective training	Phase four Sustainment training
<b>Training standards established by</b>	Services or by a joint organization (e.g. signals intelligence training standards are set by the National Security Agency).	U.S. Cyber Command	U.S. Cyber Command	U.S. Cyber Command
<b>Training administered by</b>	Services	U.S. Cyber Command vendors, such as the Defense Cyber Investigations Training Academy. Some services also have the U.S. Cyber Command's approval to deliver training.	Services at the unit level.	Services at the unit level and U.S. Cyber Command vendors.
<b>Description</b>	Provides initial specialty occupation training.	Prepares personnel for the specific position they will fill in the CMF team to which they are assigned using a particular progression of courses.	Prepares personnel to pass U.S. Cyber Command's certification standards through on-the-job training and exercises.	Refreshes team skills and certifications using activities from phases two and three. Also includes mission rehearsal exercises.

Source: GAO analysis of Department of Defense information. | GAO-19-362

Figure 5. Cyber Mission Force Training Phase Model

To support robust personnel selection, there is a lack of knowledge regarding which characteristics are held by successful and competent cyber warriors. The following portion of this literature review will analyze the purpose of the cyber career field as it currently operates, along with exploring any underlying characteristics that cyber personnel develop and demonstrate.

The DoD defines cyberspace as “the domain within the information environment that consists of the interdependent network of information technology (IT) infrastructures and resident data. It includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Cyberspace operations (CO) is the employment of

cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace”, (DoD Joint publication 3-12 cyberspace operations, 2018). The proliferation of cyber attacks has posed a growing threat to government entities, business organizations, and individuals on a national and global level.

With such a broad risk posed from a lack of cyber security, there is a high need for educated professionals to mitigate these risks. This necessity is compounded by the demand for professionals capable of performing offensive operations, including techniques that are critical for modern warfare and superiority. However, there is a major shortage in these professionals that has led to a “human capital crisis in cybersecurity” (Evans & Reeder, 2010). In 2010, the founding director of the CIA’s Clandestine Information Technology Office, Jim Gosler stated that, “There are about 1,000 security people in the US who have the specialized security skills to operate at world-class levels in cyberspace – we need 10,000 to 30,000.” At the time Gosler made this claim, U.S. Cyber Command was a sub-unified command operating under U.S. Strategic Command. In May of 2018, Cyber Command was established as a unified combatant command, CYBERCOM, which was aimed at allowing the department to grow and streamline operations under a single commander (Lange, 2018). However, the Cyber Mission Force has only grown to 6,200 members, far below the projected requirement.

With a low retention rate and a clear gap between the need for cyber workers and the quantity of those in the field, the cyber realm must make the most of the workforce that is available. While there has been little to no significant research regarding suspicion’s role in the capabilities of cyber personnel, there has been a growing amount of research in the past years aiming to uncover other common characteristics that are attributed to workers in numerous cyber fields. The findings include a mix of technical skills, those that are able to be taught and

reinforced through curriculum, along with soft skills that cannot be as easily learned such as communication, the ability to understand policy, and relationship building (Haney & Lutters, 2017).

Research was conducted to examine the personality traits of individuals who entered into a cybersecurity competition, comparing the competition's participants to individuals not employed or involved in cyberspace security. The study found that on a Big Five personality scale, competitors scored significantly higher in Openness and Agreeableness and significantly lower in the dimension of Neuroticism (Wee, Bashir, Lambert, & Guo, 2016). High levels of openness were attributed to high levels of creativity, a drive to tackle unique challenges, and the ability to think about abstract concepts. High levels of agreeableness are attributed to taking an interest in other's opinions of oneself, feeling empathy for others, and finding enjoyment in assisting others. Low levels of neuroticism are typically attributed to having emotional stability and the ability to handle stress (Pervin & John, 1999). It is possible that these cyber workers have a strong ability to think in an abstract manner along with a keen sense for the motives of others, two attributes that allow them to suspect when certain behavior is being construed. Their low levels of neuroticism could also allow them to respond to the uncertainty of these threats in a rapid manner.

In an additional field of study, information technology (IT) professionals working in security management teams were interviewed to assess their skills, responsibilities, and characteristics (Botta et al., 2007). The study found that overwhelmingly, those in the workplace were strongly characterized by three driving characteristics, the first being a strong sense for inferential analysis. The workers described examples such as having a knack for finding what crashes a system, explaining why certain technology combinations are successful, resolving

Internet Protocol address issues, etc. The next characteristic involved pattern recognition. These descriptions included things such as recognizing anomalies, mentally separating relevant from irrelevant information, and correctly hypothesizing the presence of malicious intent. The final driving characteristic is bricolage, otherwise described as constructing infrastructure or ideas from a diverse range of information. The workers were noted as describing times when they would test technology and get machines working based on a trial and error method, without a reasonable explanation as to why certain events were successful. Interviewees repeatedly claimed that they would “play” with technology and appraise different outcomes to identify problems.

While the study of suspicion as an attribute of cyber personnel is a topic that is only beginning to receive attention as an area of interest, the research conducted thus far overwhelmingly agrees that suspicion is comprised of a sense of uncertainty, the detection of malicious intent, and increased rates of cognitive activity. Aforementioned studies also conclude that cybersecurity competitors and IT professionals are often creative and abstract thinkers with the ability to face challenges as puzzles rather than as stressful hindrances to their performance. When considering the results of these studies in their entirety, perhaps the findings represent a cohesive conclusion that illustrates the thought processes of individuals who are highly competent in cyber operations. When individuals are faced with the presence of missing information and patterns of negative discrepancy, they must act in a creative manner to identify the malicious intent behind an action. This creative processing can be the result of enhanced levels of cognitive activity as the individual interprets cues and information from their environment. These individuals may act in a manner as not to alleviate stressors but to solve intriguing problems in hopes of reaping an immediate outcome. These attributes and processes

that are present in cyber operators closely align with the development of how an individual manages a suspicious situation in his or her environment.

## **2.4 Summary**

In consideration of the research regarding human suspicion, this analysis served to review current knowledge on how suspicion arises and the effects of such suspicion. It first defined the different facets of suspicion and then the stages which a person goes through to act upon their suspicion. This paper then reviewed current literature regarding the cyber career field. It talked about the current state of the Cyber Force in the DoD, to include its major labor shortage. It then reviewed which attributes have been studied in cyber workers and how these attributes relate back to the concept of suspicion.

### **III. Methodology**

#### **3.1 Chapter Overview**

This chapter introduces the methodology and design implemented to address the previously stated research questions stated in Section 1.4. It provides a description of the surveys and performance measures that were administered, the environment in which the research was conducted, and the individuals who participated in this study. This chapter also provides a brief overview of the Cyber 200 and 300 courses of which a portion of the study's participants were students.

#### **3.2 Participants**

To gain a preliminary baseline measurement of suspicion levels amongst individuals who the Air Force categorizes as experts in the cyber career field, the surveys were first administered to 57 students upon the completion of Cyberspace Professional Continuing Education Courses, otherwise known as Cyber 200 and 300. The courses occurred in the Air Force Cyberspace Technical Center of Excellence within the Air Force Institute of Technology, Wright-Patterson Air Force Base. Participants consisted of officer and enlisted active duty personnel all within the Cyber Professional Workforce. The courses hold a prerequisite of eight career years in the field, with the students who completed the Suspicion Propensity Index having cyber experience ranging from 10 to 37 years ( $M = 22.8$ ,  $SD = 7.25$ ). Students enrolled in these courses are deemed highly competent by their career field and must be nominated to partake in this advanced training based on their abilities. The courses are far beyond introductory level and are held for top-performing cyber operators in an effort to maintain the expertise and competences necessary to triumph in future cyberspace conflicts.

In addition to the collection of baseline measurements from cyber personnel, data was collected from members of other career fields within the DoD having little to no cyber experience. These participants included officer and enlisted Air Force at the Air Force Institute of Technology (AFIT). These non-cyber participants were a mixture of students pursuing master's degrees and other certificates offered at the university. The SPI, a trust measurement, and a Mission Scenario Questionnaire were administered to 65 participants ranging from 1 to 30 years of government work experience ( $M = 8.93$ ,  $SD = 8.06$ ).

Prior to beginning data collection, Cohen's Power Primer (Cohen, 1992) was referenced to gain an estimate of recommended sample size for statistical relevance. Based on a power = 0.80 and an alpha of 0.05, a necessary sample size of at least 64 was needed for a medium effect. With a total of 122 total participants (57 cyber and 65 non-cyber), this requirement was met.

### **3.3 Measures**

As it has been proven by past studies, suspicion consists of three major components: cognitive activity, perception of malicious intent, and uncertainty (Bobko et al., 2014). All three must be present simultaneously for an individual to experience suspicion; therefore, the measure of suspicion must be derived through performance and outcome measures. Table 1 depicts the three measures that were used in this study, along with their number of data points (per participant), and the scale of each measure. In addition to these measurements, a demographics



questionnaire was administered to collect characteristics of the participants. The demographics questionnaire is shown in Appendix A.

*Table 1. Measurements Questionnaires*

<b>Measurement</b>	<b>Source</b>	<b>Number of Items</b>	<b>Scale</b>
Trust	Mayer, Davis, & Schoorman, 1995	8	Likert 1-7
Suspicion Propensity Index (SPI)	Bobko et al., 2014	44	Likert 1-5
Mission Performance Questionnaire	Adapted with JSOC Cyber Special Missions Flt/CC	6	0-6

To conduct the measurement of suspicion levels amongst the subjects, the Suspicion Propensity Index was administered on a voluntary basis to the Cyber 200 and 300 students, along with non-cyber participants at the Air Force Institute of Technology. The SPI contained eleven situation-based items. Each scenario contained four responses with each response coded to represent one of the following indicators: trust, uncertainty and cognitive activity, paranoia, and uncertainty and perceived malintent. Each response was individually scored on a scale of one through five, with one being “not at all accurate” and five being “very accurate.” In total, the eleven scenarios and four responses per item provided 44 data points per participants. The Suspicion Propensity Index can be viewed in its entirety in Appendix B.

As Bobko et al. (2014) proposed that one's propensity to trust is a factor of one's capacity to become suspicious- and in consideration of the contested research regarding trust's relationship to suspicion, trust was the next attribute to be measured amongst the AFIT student participants. As one of the most highly accepted and utilized questionnaires in academia, Mayer's eight-item propensity to trust questionnaire was used for the trust measurement (Mayer, Davis, and Schoorman, 1995). The eight items of the questionnaire were scored on a scale of one to seven, with one being "strongly disagree" and seven being "strongly agree." The questionnaire can be viewed in its entirety in Appendix C.

In order to measure performance in cyber operations, participants completed a six-scenario questionnaire used to measure general inclinations regarding the recognition and response to potential cyber threats. The scenarios were adapted from an already-existing set of training scenarios that are utilized by cyber mission defense teams across Air Education and Training Command (AETC) bases. The scenarios were provided by the Cyber Special Missions Flight at Joint Special Operations Command (JSOC). AETC uses these scenarios are representative of relevant and current cyber threats, and provide opportunity to assess and train cyber forces ensuring their continuation of knowledge and training. The scenarios were contained in a questionnaire containing a description of the situation along with three potential responses to that situation. While the items were carefully constructed to trigger the participants' use of judgement, each scenario ultimately had only one correct action response. The questionnaire can be viewed in Appendix D.

### 3.4 Procedure

The primary focus of this research is to investigate how an individual's capabilities in cyber operations are affected by her or his propensity for suspicion, along with how suspicion levels differ amongst individuals with different experience levels and varying career fields. To capture variety within a sample population of non-cyber individuals, the questionnaire measures were administered on a voluntary basis to students at the Air Force Institute of Technology, differing in age and coming from a wide assortment of career and educational fields other than the cyber career field. The participants first took the demographics questionnaire (Appendix A), followed by the SPI (Appendix B), trust measurement questionnaire (Appendix C), and mission scenario questionnaire (Appendix D). While the demographics questionnaire collects information regarding the background of the participants, their names were not recorded, and their responses were thus anonymous. The surveys were collected at large from the students to ensure their anonymity and were scored using a participant identification number.

In order to capture variety within a sample of individuals within the cyber career field, the questionnaires were administered on an optional basis to students upon completion of the Cyber 200 and 300 courses, also taking place at the Air Force Institute of Technology. Each course has a three-week duration and occurs roughly every month. The data was collected from courses that were conducted between April and October of 2019, and the survey was offered on the last day of the course upon completion. Overall, 122 individuals participated in the study from the cyber and non-cyber populations.

### **3.5 Analysis Overview**

This experiment's data was analyzed using multiple techniques. First, descriptive statistics were used to overview basic trends and relationships within the data. A basic Pearson Correlation table was used to investigate the statistical association between variables to include the performance measure assessment, total SPI score, total Mayer's trust questionnaire score, career (cyber vs. non-cyber), years in military service, and the individual entities of the SPI to include trust, cognitive activation, paranoia, and uncertainty and malintent. Next, linear regression was performed to determine the strength of a statistical relationship between SPI scores and mission performance questionnaire scores (RH-1). To compare the general means of SPI scores for cyber operators and non-cyber operators (RH-2), a one-sample T-Test was used to explore differences among the two populations. In order to investigate the relationship between years of experience and SPI scores (RH-3), a basic Pearson Correlation table was used to correlate the two variables. A general linear model was also used to observe the effects of the interaction between years of experience and career on suspicion scores. Finally, to explore the relationship between trust and both suspicion and cyber performance (RH-4), multiple linear regression was performed to determine the trust questionnaires' capacity to predict performance scores, along with multiple linear regression to determine the combined capacity of trust and SPI scores to predict performance.

### **3.6 Summary**

This chapter provided an overview of the design and methodology used within this research. It discussed the distribution of the surveys, the environment in which the surveys were taken, the participants who completed the surveys, as well as an overview of the Cyber 200 and 300 courses in which a portion of the students were enrolled.

## IV. Analysis and Results

### 4.1 Chapter Overview

This chapter provides an overview of the descriptive and statistical analysis conducted on the experimental data. It reflects upon the different research questions that encompass the goals of this study, along with the results of the research conducted.

### 4.2 Performance Measurement

The performance measurement used in this study, the cyber mission performance questionnaire, was scored on a scale of 1-6. To verify the validity of the measure, descriptive statistics were applied along with an independent samples T-Test comparing the scores across both sample populations. The T-Test displayed in Table 3 reveals that the mean performance scores of cyber personnel are significantly different than the performance scores among non-cyber personnel ( $p = 0.011$ ) with a mean difference of 2.364. Overall, results across the cyber participants ( $M = 5.33$ ) were higher than results across the non-cyber participants ( $M = 2.97$ ).

Table 2. Performance mean comparison among non-cyber (0) and cyber (1) populations.

Group Statistics					
	Career	N	Mean	Std. Deviation	Std. Error Mean
Perf Score	0	65	2.97	1.060	.132
	1	57	5.33	.636	.084

**Independent Samples Test**

	Levene's Test for Equality of Variances		t-test for Equality of Means						
	F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
								Lower	Upper
Performance Score	6.691	.011	-15.136	106.776	.000	-2.364	.156	-2.674	-2.054

### 4.3 Descriptive Statistics & Correlations

For this analysis, all variables were continuous with the exception of “Career,” which was coded as a categorical dichotomous variable with 0 representing non-cyber personnel and 1 representing cyber personnel. Table 3 displays the descriptive statistics for the data collected. As shown in the table, the mean years of service among the cyber personnel was much higher than that of the non-cyber participants. Both populations display a large standard deviation, indicating a wide range of years of service among the cyber and non-cyber personnel.

*Table 3. Descriptive Statistics*

	N	Minimum	Maximum	Mean	Std. Deviation
Perf Score	122	1	6	4.07	1.478
SPI Total	122	41	91	64.20	9.432
Trust Total	122	19	42	28.54	5.415
Years in Service Cyber	57	10.00	37.00	22.8070	7.25416
Years in Service Non-Cyber	65	1.00	30.00	8.9308	8.05638

Table 4 displays the correlations among all variables. Among key variable relationships are years in service and performance ( $r = 0.558, p < 0.0001$ ), total SPI scores and Mayer’s trust

scores ( $r = -0.244$ ,  $p = 0.007$ ), total SPI scores and performance ( $r = 0.541$ ,  $p < 0.0001$ ), and Mayer's trust scores and performance ( $r = -0.313$ ,  $p < 0.0001$ ). It should also be noted that certain individual facets of the total SPI score are strongly correlated with performance. These include paranoia ( $r = 0.435$ ,  $p = 0.001$ ) and uncertainty/malintent ( $r = 0.595$ ,  $p < 0.0001$ ). Correlations will be discussed in greater detail throughout the remainder of this chapter.

Table 4. Correlations for all variables. Values for SPI Total and SPI subscale scores are shown, including the paranoia (PAR), uncertainty/malintent (UNMI) and cognitive activation (CA) subscale scores.

		Career	Yrs in Service	Perf Score	SPI Trust	SPI PAR	SPI UN/MI	SPI CA	SPI Total	Mayer's Trust Total
Career	Pearson Corr	1	.628**	.810**	-.290**	.350**	.609**	.332**	.552**	-.432**
	Sig.		.000	.000	.001	.000	.000	.000	.000	.000
	N	122	122	122	122	122	122	122	122	122
Yrs. in Service	Pearson Corr	.628**	1	.558**	-.322**	.301**	.618**	.304**	.543**	-.422**
	Sig.	.000		.000	.000	.001	.000	.001	.000	.000
	N	122	122	122	122	122	122	122	122	122
Performance Score	Pearson Corr	.810**	.558**	1	-.194*	.435**	.595**	.328**	.541**	-.313**
	Sig.	.000	.000		.032	.000	.000	.000	.000	.000
	N	122	122	122	122	122	122	122	122	122
SPI Trust	Pearson Corr	-.290**	-.322**	-.194*	1	.015	-.144	-.073	-.128	.488**
	Sig.	.001	.000	.032		.870	.113	.424	.160	.000
	N	122	122	122	122	122	122	122	122	122
SPI PAR	Pearson Corr	.350**	.301**	.435**	.015	1	.678**	.388**	.625**	-.144
	Sig.	.000	.001	.000	.870		.000	.000	.000	.114
	N	122	122	122	122	122	122	122	122	122
SPI UN/MI	Pearson Corr	.609**	.618**	.595**	-.144	.678**	1	.508**	.887**	-.267**
	Sig.	.000	.000	.000	.113	.000		.000	.000	.003
	N	122	122	122	122	122	122	122	122	122
SPI CA	Pearson Corr	.332**	.304**	.328**	-.073	.388**	.508**	1	.848**	-.148
	Sig.	.000	.001	.000	.424	.000	.000		.000	.104
	N	122	122	122	122	122	122	122	122	122
SPI Total	Pearson Corr	.552**	.543**	.541**	-.128	.625**	.887**	.848**	1	-.244**
	Sig.	.000	.000	.000	.160	.000	.000	.000		.007
	N	122	122	122	122	122	122	122	122	122
Trust Total	Pearson Corr	-.432**	-.422**	-.313**	.488**	-.144	-.267**	-.148	-.244**	1
	Sig.	.000	.000	.000	.000	.114	.003	.104	.007	
	N	122	122	122	122	122	122	122	122	122

\*\* . Correlation is significant at the 0.01 level (2-tailed).

\* . Correlation is significant at the 0.05 level (2-tailed).



#### 4.4 Suspicion and Performance

To recall from section 1.5.1, RH-1 claims that an individual's SPI score will be positively correlated to their mission performance score. Figure 6 displays the distributions of performance scores among both the cyber and non-cyber populations, indicated by individual scores on the cyber mission performance questionnaire.

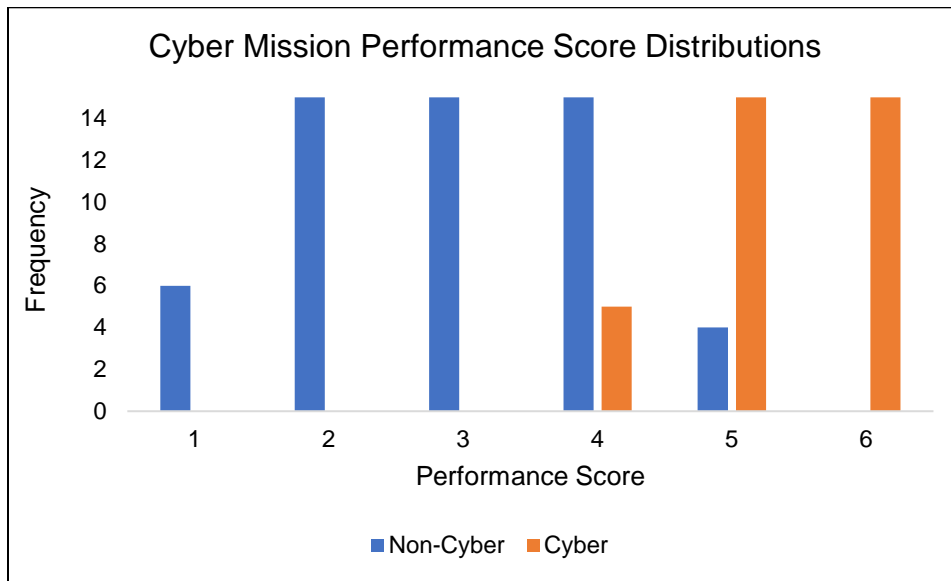


Figure 6. Distribution of performance scores among cyber and non-cyber personnel.

As shown in Table 4, mission performance and SPI score have a correlation of 0.541 ( $p < 0.0001$ ). To further this analysis, linear regression was performed with SPI score as the predictor for the dependent variable of mission performance. As shown in Table 3, there was a large amount of variation between the years in service for the different career field categories. Further, there was a significant difference in years of service between the career field categories. Members of the cyber career field averaged 22.81 years of service ( $SD = 7.25$ ) while non-cyber individuals averaged 8.93 years of service ( $SD = 8.1$ ). To ensure that this difference between populations did not bias the SPI results, the model controlled for years in service prior to performing the analysis.

The model summary displays the R and R<sup>2</sup> goodness of fit measures for the model, showing that years of service accounts for 31.2% of the variance in an individual's performance score. R<sup>2</sup> increases in the second model, which includes SPI score as well as years in service. As shown, the model which includes the SPI scores accounts for 39.2% of the variance in performance scores. The change in R<sup>2</sup> with the addition of SPI as a predictor amounts to 0.08 (F(1,119) = 15.76, p < 0.0001) indicating that the models, with and without the SPI, are statistically different. A T-test conducted on each predictor within the regression model indicated that the SPI accounted for a statistically significant portion of the variance in the performance score (t(1,120) = 3.97, p < 0.0001). The coefficients table displays values of the overall regression equation, with Performance Score = -0.15 + 0.054(Years in Service) + 0.053(SPI Score). The results displayed in Table 5 indicate that the total SPI score has a significant effect on performance score after controlling for years in service (p < 0.0001). Both the "Years in Service" and "SPI Total" variables have a positive influence on the dependent variable "Performance Score."

Table 5. SPI as predictor for performance score.

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.558 <sup>a</sup>	.312	.306	1.231	.312	54.325	1	120	.000
2	.626 <sup>b</sup>	.392	.382	1.162	.080	15.759	1	119	.000

a. Predictors: (Constant), Yrs in Service

b. Predictors: (Constant), Yrs in Service, SPI Total

**ANOVA<sup>c</sup>**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.375	1	82.375	54.325	.000 <sup>a</sup>
	Residual	181.961	120	1.516		
	Total	264.336	121			
2	Regression	103.654	2	51.827	38.383	.000 <sup>b</sup>
	Residual	160.682	119	1.350		
	Total	264.336	121			

- a. Predictors: (Constant), Yrs in Service  
 b. Predictors: (Constant), Yrs in Service, SPI Total  
 c. Dependent Variable: Perf Score

**Coefficients<sup>a</sup>**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.844	.201		14.177	.000
	Yrs in Service	.080	.011	.558	7.371	.000
2	(Constant)	-.150	.778		-.193	.847
	Yrs in Service	.054	.012	.375	4.404	.000
	SPI Total	.053	.013	.338	3.970	.000

- a. Dependent Variable: Perf Score

#### 4.5 Suspicion among Cyber vs Non-Cyber Personnel

Section 1.5.2 states that cyber operators will yield higher SPI scores in comparison to non-cyber personnel (RH-2). To test this hypothesis, an independent samples T-Test was performed on the SPI scores of cyber and non-cyber personnel. The mean SPI score for non-cyber operators (M = 59.45, SD = 8.06) was lower than the mean SPI score for cyber operators (M = 69.61, SD = 7.87). Table 6 displays these results, indicating that the means are significantly different ( $t(1,120) = 7.029, p < 0.0001$ ).

Table 6. Cyber and non-cyber SPI scores.

Group Statistics				
	N	Mean	Std. Deviation	Std. Error Mean
SPI Score Non-Cyber	65	59.45	8.058	1.000
SPI Score Cyber	57	69.61	7.871	1.043

Independent Samples Test										
		Levene's Test for Equality of Variances		t-test for Equality of Means						
		F	Sig.	t	df	Sig. (2-tailed)	Mean Difference	Std. Error Difference	95% Confidence Interval of the Difference	
									Lower	Upper
SPI Total	Equal variances assumed	.093	.762	-7.029	120	.000	-10.168	1.447	-13.032	-7.304
	Equal variances not assumed			-7.040	118.590	.000	-10.168	1.444	-13.028	-7.308

Figure 7 displays the separate distributions of SPI scores for the cyber and non-cyber populations. As shown in the distributions, the scores of those in cyber are shifted to the right of non-cyber personnel SPI scores.

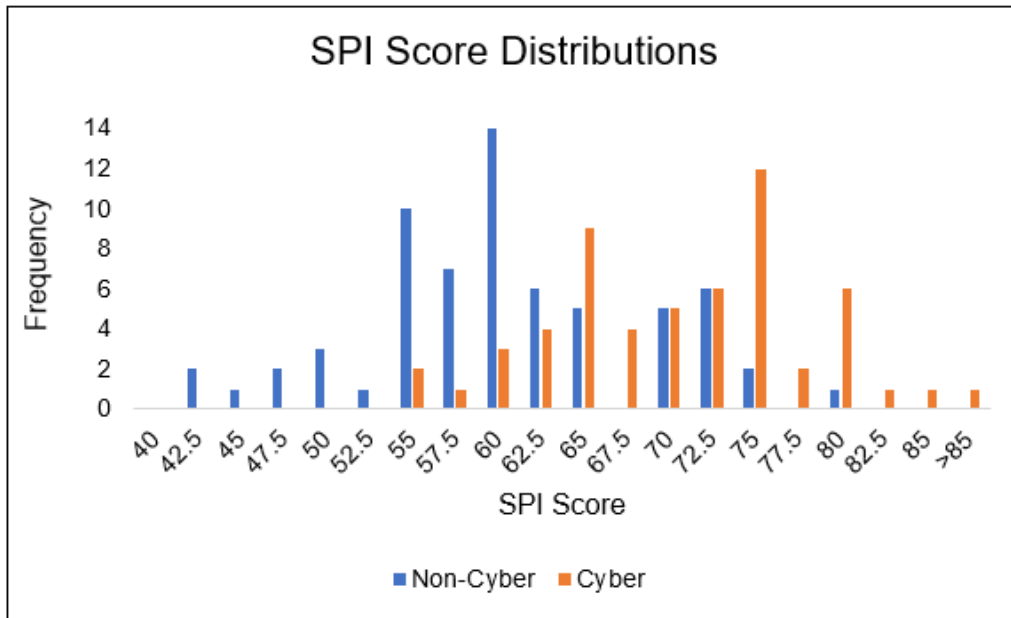


Figure 7. Distribution of SPI scores among cyber and non-cyber personnel.

#### 4.6 Effects of Years of Experience

In consideration of section 1.5.3, RH-3 presumes that years of experience will have a positive correlation to an individual's SPI score, and that the correlation will be more prominent among cyber operators than among non-cyber operators. As shown in Table 4, the correlation between total SPI score and years in service is 0.543, which is significantly greater than zero ( $p < 0.0001$ ). A general linear model procedure was used to view the effects of both years in service and career on suspicion scores, along with the effect of their interaction. As shown in Table 7, the interaction between career and years in service had a significant effect ( $F(1,118) = 5.92$ ,  $MSE = 56.4$ ,  $p = 0.016$ ) on the dependent variable of SPI total score. Figure 8 provides a visual depiction of the interaction's effect, displaying the modeled relationship between total SPI scores and years in service while moderated by career. Within the interaction plot, non-cyber and cyber personnel have similar suspicion levels for less years in service. However, as participants gain

experience, suspicion levels show a greater differentiation between the cyber and non-cyber sample populations.

Table 7. Interaction between years in service and career on suspicion scores.

**Tests of Between-Subjects Effects**

Dependent Variable: SPI Total

Source	Type III Sum of Squares	df	Mean Square	F	Sig.
Corrected Model	4109.872 <sup>a</sup>	3	1369.957	24.289	.000
Intercept	98624.391	1	98624.391	1748.605	.000
Career	9.681	1	9.681	.172	.679
YrsinService	56.629	1	56.629	1.004	.318
Career * YrsinService	333.777	1	333.777	5.918	.016
Error	6655.407	118	56.402		
Total	513554.000	122			
Corrected Total	10765.279	121			

a. R Squared = .382 (Adjusted R Squared = .366)

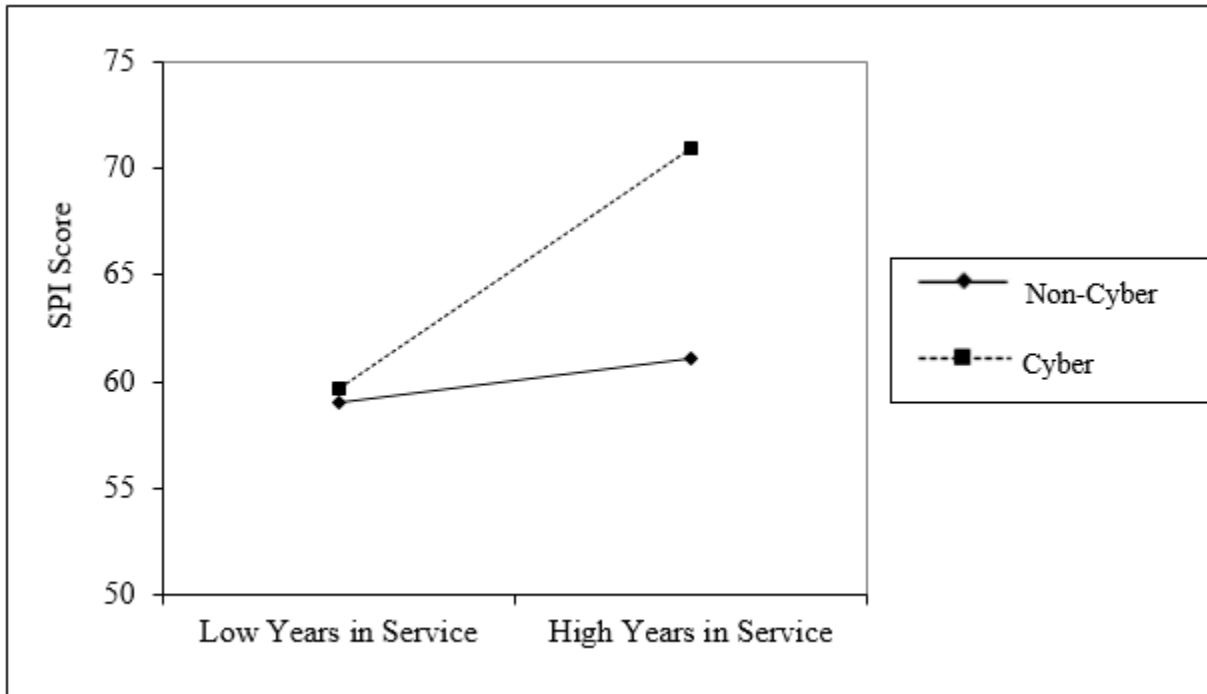


Figure 8. Model results for the two-way interaction between career and years in service on total SPI scores.

#### 4.7 Trust and Performance

As shown in Table 4, the correlation between Mayer's trust scale and mission performance is -0.313, which is again statistically different from zero ( $p < 0.0001$ ). Linear regression was performed, investigating the predictive capability of the trust measure on cyber mission performance. As before, years of service alone accounts for 31.2% of the variance in performance scores, while a model including years in service and the trust measurement account for 31.9% of the variance. This change is insignificant ( $t(1,119) = -1.123, p = 0.264$ ) indicating that after controlling for years of service, the trust measurement did not have a significant effect on performance on the cyber mission questionnaire. Results can be observed in Table 8.

Table 8. Trust measurement as a predictor for performance.

**Model Summary**

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.558 <sup>a</sup>	.312	.306	1.231	.312	54.325	1	120	.000
2	.565 <sup>b</sup>	.319	.307	1.230	.007	1.260	1	119	.264

a. Predictors: (Constant), Yrs in Service

b. Predictors: (Constant), Yrs in Service, Trust Total

**ANOVA<sup>c</sup>**

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.375	1	82.375	54.325	.000 <sup>a</sup>
	Residual	181.961	120	1.516		
	Total	264.336	121			
2	Regression	84.282	2	42.141	27.852	.000 <sup>b</sup>
	Residual	180.054	119	1.513		
	Total	264.336	121			

a. Predictors: (Constant), Yrs in Service

b. Predictors: (Constant), Yrs in Service, Trust Total

c. Dependent Variable: Perf Score

**Coefficients<sup>a</sup>**

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.844	.201		14.177	.000
	Yrs in Service	.080	.011	.558	7.371	.000
2	(Constant)	3.661	.755		4.850	.000
	Yrs in Service	.074	.012	.519	6.214	.000
	Trust Total	-.026	.023	-.094	-1.123	.264

a. Dependent Variable: Perf Score

Multiple linear regression was also performed to observe the explanatory variables of trust and total SPI score, showing their combined effect at predicting the total mission performance score after controlling for years of service. Together, trust and suspicion account for 39.8% of the variance within the cyber mission performance questionnaire. The F-test is significant ( $p < 0.0001$ ), thus it can be assumed that the model explains significant variance in



cyber mission performance scores. However, the coefficients table shows that the trust parameter does not have statistical significance on the model results ( $t(1,118) = -1.115, p = 0.267$ ). The results can be observed in Table 9.

Table 9. Predictive capability of the combined effect of trust and suspicion.

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.558 <sup>a</sup>	.312	.306	1.231	.312	54.325	1	120	.000
2	.631 <sup>b</sup>	.398	.383	1.161	.087	8.517	2	118	.000

a. Predictors: (Constant), Yrs in Service

b. Predictors: (Constant), Yrs in Service, Trust Total, SPI Total

#### ANOVA<sup>c</sup>

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	82.375	1	82.375	54.325	.000 <sup>a</sup>
	Residual	181.961	120	1.516		
	Total	264.336	121			
2	Regression	105.328	3	35.109	26.055	.000 <sup>b</sup>
	Residual	159.008	118	1.348		
	Total	264.336	121			

a. Predictors: (Constant), Yrs in Service

b. Predictors: (Constant), Yrs in Service, Trust Total, SPI Total

c. Dependent Variable: Perf Score

#### Coefficients<sup>a</sup>

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	2.844	.201		14.177	.000
	Yrs in Service	.080	.011	.558	7.371	.000
2	(Constant)	.631	1.047		.603	.548
	Yrs in Service	.048	.013	.339	3.722	.000
	Trust Total	-.024	.022	-.088	-1.115	.267
	SPI Total	.053	.013	.336	3.952	.000

a. Dependent Variable: Perf Score

## 4.8 Summary

This chapter presented the data analysis and results pertaining to relevant research questions and hypotheses. It covered the statistical tests performed in order to investigate each hypothesis, along with additional exploratory tests that were conducted.

## V. Conclusions and Recommendations

### 5.1 Chapter Overview

This chapter will first summarize the conducted research, along with the interpretation and significance of the results. It will then discuss recommendations for action regarding the findings, along with addressing the potential for future work in this realm of research.

### 5.2 Evaluation of Research Questions

This section will review the initial research questions and draw conclusions based on the data analysis.

- *RQ-1: Is an individual's level of suspicion correlated to his or her success within the cyberspace career field?*

The correlation analysis supported this hypothesis by demonstrating that suspicion and mission performance have a significant correlation of 0.541. While accounting for differences in years of service among the two sample populations, the SPI scores accounted for 39.2% of variation within participants' mission performance scores. Across both the cyber and non-cyber groups, it can be concluded that high levels of suspicion are correlated with one's ability to perform well on the cyber mission performance questionnaire. However, differences in suspicion scores prove to be much lower among the two populations for individuals early in their careers and increases significantly as time within the cyber career field increases. Overall, performance in the cyberspace career field does have a positive relationship with suspicion, and this relationship becomes significantly stronger with increased time in the career field.

- *RQ-2: Do current Air Force cyber operators differ in their levels of suspicion when compared to members of other career fields?*

The total SPI is calculated on a scale of 22 to 110. Participants within the cyber operator sample population had a mean score of 69.61 versus the non-cyber sample population which had a mean score of 59.45. This 10.16 point difference indicates that the sample of cyber personnel were generally more suspicious than the sample of non-cyber personnel. It should not go without recognition that general increases in suspicion over time prove much more prominent among cyber personnel than non-cyber personnel. In consideration of Bobko's Three Stage Model, training has a large impact on how an individual enters a suspicious state. Within the cyber population alone, it is possible that the training and experience that operators gain over their career plays a large role in this increase in suspicion compared to members of other career fields.

- *RQ-3: Does an Airman's years of experience in their field correlate to significant differences in levels of suspicion?*

The data presumed that for both sample populations, years of experience and suspicion scores have a significant correlation of 0.543. When observing the effects of career, years of service, and the interaction of these variables on suspicion, both non-cyber and cyber personnel had similar SPI scores among participants with lesser years in service. As years in service increased, there was a greater difference in SPI scores between the non-cyber and cyber sample populations. Cyber personnel with a large number of years in service were determined to have the highest SPI scores. It can be concluded that years of experience is positively correlated with levels of suspicion, indicating that more experienced personnel provide higher SPI scores than less experienced personnel. Furthermore, while this effect was present for both cyber and non-cyber personnel, the

effect was much stronger across the cyber personnel. Therefore, SPI scores seem to increase in conjunction with one's experience in the cyber career field.

- *RQ-4: Does an Airman's propensity to trust correlate with both her/his levels of suspicion and success within the cyberspace career field?*

The trust measurement used in this study yielded a significant correlation with cyber mission performance ( $r = -0.313$ ,  $p < 0.0001$ ). Trust also contributed to 31.9% of the variance within performance scores after controlling for years in service; however, these results do not prove to be a significant change from the explained variance by years of service alone. These results indicate that although there is a correlation between an individual's level of trust and cyber performance, this relationship is largely due to years in service as opposed to trust as an independent parameter. Further investigation shows that the trust measurement in conjunction with SPI scores account for 39.8% of variance in performance scores. This is a slight increase from the 39.2% of variance that is explained by suspicion alone while also controlling for years in service; however, the contribution made by the trust parameter to this model does not prove to be significant ( $p = 0.267$ ).

### **5.3 Significance of Research**

The findings within this research have the potential to contribute a noticeable impact on the cyber career field within the entirety of the Department of Defense. This research is the first of its kind to consider suspicion as an influencing factor on cyber performance; and opens the door for additional exploration on the subject matter. Successful members of the cyber career field demonstrated higher levels of suspicion than their non-cyber counterparts, especially with increased experience. While the findings on suspicion within this research do not provide the necessary data to formulate a screening tool into the cyber career field, the results present

important findings for the career field at large. This increase over time indicates that suspicion may be a learned attribute and can thus be utilized to train cyber personnel to be more successful within their career field. If early cyber training focuses on enhancing the suspicion of operators, these training modifications could accelerate the trend of increasing suspicion, thus improving the quality of the cyber force.

In addition to contributions in the cyber career field, the findings of this research provide insights into other academic fields that display a general lack of literature in regard to suspicion and trust. While it is accepted that both trust and suspicion play a role in the tendencies of groups and individuals, there have been few findings to prove exactly what these effects may entail or that discuss the relationship between trust and suspicion. This study investigated the theorized relationship between trust and suspicion propensity, ultimately showing that the two attributes display a moderate, yet significant, negative correlation. The significance of this correlation provides some credibility to the argument that both trust and suspicion are predicting a similar underlying phenomenon. Furthermore, this thesis showed that suspicion (as measured through the SPI) is an indicator of performance while trust (as measured with Mayer's trust measure) does not provide similar predictability. These findings can provide insight to a field that currently holds very little research, while also indicating to cyber personnel that suspicion should be a prioritized aspect of training as opposed to trust. The findings also present an opportunity for further exploration into the relationship between the attributes of trust and suspicion, along with their effect on one another, on one's personality, and performance in different career fields.

#### **5.4 Recommendations for Future Research**

The indications in this research suggest that while variability in cyber performance is partially explained by operator suspicion, there are still other attributes that contribute to success

within the career field. These results pose an opportunity for further research into additional attributes that may affect one's ability to perform well at various cyber operations. As the findings presented in this study indicated that suspicion tends to increase cyber performance as an individual acquires years of experience, a focal point of future research should lie in gaining an understanding of how suspicion changes over time. The little research on suspicion that has been conducted in the past indicates that individuals hold a propensity to become suspicious. However, this study indicates that it is a learned attribute. These conflicting findings present an opportunity for further investigation among various career fields in order to validate suspicion as a characteristic that can be learned or that individuals are predisposed to act upon.

A key revelation from these findings includes the potential for suspicion to contribute to training modifications within the cyber career field. If future research is conducted, it has the potential to identify how and why operators act upon their suspicions and how these suspicions become present in certain individuals. If these questions can be answered, they pose a potential for accelerating the development of suspicion in cyber operators and, in turn, accelerating greater levels of success within the career field. There is also still room for investigation into the specific attributes that contribute to initial success in the career field. In regard to the development of a screening tool for cyber within the Air Force, additional research can be conducted to explore which characteristics allow airmen to be successful at cyber operations. Potential factors for investigation include creativity, persistence, general curiosity, detail orientation, and analytical thinking.

In order to conduct further validation of the recently developed Suspicion Propensity Index and to answer questions regarding suspicion as an attribute, the SPI can be used to evaluate individuals undergoing initial cyber training at Keesler Air Force Base in which trainees

undergo a six-month course to successfully become operators in the cyber field. A great assessment of the SPI's predictive ability could include an initial administration of the index upon the start of cyber training. Following the course's conclusion, SPI scores could be compared to individuals' pass/fail rates, along with instructor ratings of performance. These results would further indicate suspicion's relationship with performance in the cyber field, looking at a new population of individuals just beginning their career.

Outside of the cyber realm, additional research can be conducted exploring the impact of both trust and suspicion on individuals' daily lives. While within this study the two attributes proved to have an inverse relationship, further investigation into the effect of this relationship would benefit other areas of academia. For example, one could look at suspicion and trust propensity in terms of their effects on correspondence bias, the formation and maintenance of personal relationships, workplace interactions, and attributional thinking.

## **5.5 Summary**

In summary, this research is applicable to the large-scale DoD challenge of training individuals to be successful within the cyber career field. Through the novel investigation of suspicion as a predictor for improving cyber capabilities, this research provides an initial step to modifying the training tools utilized by cyber personnel in the Air Force and other branches of the United States military. While there is still a vast amount of research that should be conducted to bolster the findings of this thesis, the results have the capacity for a long-term influence on the cyber career field and military operations at large.



## Appendix A: Demographics Questionnaire

1. Please indicate your age: \_\_\_\_\_
2. Please indicate your gender: Male \_\_\_\_\_ Female \_\_\_\_\_
3. Please answer the following statements regarding your previous education:
  - a. Highest level of education previously achieved:  
High School \_\_\_\_\_ Some College \_\_\_\_\_ Bachelors \_\_\_\_\_ Master's \_\_\_\_\_ Ph.D. \_\_\_\_\_
  - b. Previous education major: \_\_\_\_\_
  - c. Indicate your GPA for the highest level of education achieved: \_\_\_\_\_
  - d. Indicate how many cyber courses have you completed over your academic career (programming, security, engineering, etc.): \_\_\_\_\_
4. If currently attending school, please answer the following statements:
  - a. Indicate the level of education you are currently pursuing:  
Certificate \_\_\_\_\_ Masters \_\_\_\_\_ Ph.D. \_\_\_\_\_ Other (specify): \_\_\_\_\_
  - b. Indicate your current major: \_\_\_\_\_
  - c. Indicate your current GPA: \_\_\_\_\_
  - d. GRE Score (if applicable): \_\_\_\_\_
5. Please answer the following statements regarding your work experiences:
  - a. Indicate your primary career field occupation: \_\_\_\_\_
  - b. Indicate number of years' experience in primary career field: \_\_\_\_\_
6. Please indicate your employment category: Military \_\_\_\_\_ Civilian \_\_\_\_\_
  - a. If military,
    - i. Indicate your current rank: \_\_\_\_\_
    - ii. Indicate total years in service: \_\_\_\_\_
  - b. If civilian,
    - i. Indicate employment sub-category:  
Government \_\_\_\_\_ Contractor \_\_\_\_\_ Other \_\_\_\_\_
    - ii. Indicate total years in sub-category: \_\_\_\_\_
    - iii. If prior military, indicate number of years in military service: \_\_\_\_\_

## Appendix B: Suspicion Propensity Index

Purpose: The purpose of this questionnaire is to gain insights into your general inclination towards the others and/or the actions of others.

Instructions: For the following scenarios, please read the description and indicate how accurately each of the response statements describes you.

### Scenario 1.

Imagine you have applied for a job, for which you are qualified, and have gone through the interview process. Shortly after the interview, you receive notification that the company decided to offer the job to another individual.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would decide to move on and continue searching for a job.					
b. I would follow up with someone at the company and request more information about why I wasn't chosen.					
c. I would be certain that someone I was in contact with during the process must not like me, and I would do something like telling others to avoid this company.					
d. I would wonder if there was someone at the company who I had contact with who purposely wanted to keep me from getting the job.					

### Scenario 2.

Imagine that you see a discussion on a social networking website indicating that several of your friends got together this past weekend, and they didn't contact you about joining them.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would be certain that my friends purposefully excluded me, and I would do something such as refuse to continue socially interacting with them.					
b. I would not dwell on it, and instead focus my thoughts on something else.					
c. I would search for more information and reasons as to why they might have gotten together and not contact me (such as an invitation by someone I'm not friends with).					
d. I would wonder if one of them excluded me on purpose.					

**Scenario 3.**

Imagine you are interested in buying a new car and are in a car showroom. After telling a salesperson you are interested in a mid-level model, he says, “In the long run, a high-end model with the extra options is a better investment.”	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would look around and listen to see if other customers were receiving the same advice from the salespeople.					
b. I would wonder if the salesperson was only interested in the potential increase in the commission from the sale.					
c. I would be certain that the salesperson is not truly trying to help me, and I would do something such as leave and never return to that dealership.					
d. I would accept the help – it’s always nice to have an expert opinion.					

**Scenario 4.**

Imagine you enter a contest for a local school’s fundraiser to guess the number of marbles in a large jar. The prize is a \$100 gift card to a popular online store. After making your best guess, you find out the following week that you did not win and that one of the teachers at the school won the contest.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would wonder if the teacher who won had cheated and/or had gotten inside information on this activity.					
b. I would accept another person winning – better luck next time.					
c. I would think about flaws in my own thinking (e.g., flaws in how I came up with my estimate) that might explain why I didn’t win.)					
d. I would be certain that the contest was rigged, and I would do something such as never participate in that school’s fundraisers again.					

### Scenario 5.

Imagine that you have a teenage son. He comes home a half hour <u>before</u> curfew and heads straight to his room without stopping to talk to you. In the past he always has checked in with you when arriving home, and he has never returned home before curfew.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would assume he is tired and probably just didn't feel like stopping to talk to me.					
b. I would wonder what he might be hiding from me. ( <b>high agreement indicates uncertainty and perceived malintent</b> )					
c. I would be certain that he is hiding something from me, and I would do something such as taking away his driving privileges without discussing it further with him.					
d. I would go to his room and attempt to find out what might be wrong.					

### Scenario 6.

Imagine you have just visited an online store to shop for a book you want to purchase. After finding the book you want on a discount website that you haven't heard of before, you decide to go ahead and purchase the book. After entering your credit card information and clicking the "confirm purchase" button, you wait for an email confirmation of your purchase. However, the email confirmation never arrives.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would be certain that the lack of email confirmation meant that I had lost the money, and I would do something such as immediately cancel my credit card or not shop online in the future.					
b. I would try to email the company to determine if the purchase was confirmed, and I would attempt to find out more information about the company.					
c. I would wonder if there was any danger in providing my credit card information.					
d. I would wait a few days to see if the confirmation is delivered as the website promised.					

**Scenario 7.**

Imagine you start working for a new company and are told by your supervisor that you will receive a raise within the first 3 months. After 5 months, you haven't received a raise. When you ask, your supervisor keeps telling you "we're working on it."	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would try to get more information (e.g., Did coworkers get their raises on time? Is the company doing okay financially?)					
b. I would be certain that my supervisor is trying to avoid paying me the raise I deserve, and I would do something such as consider quitting.					
c. I would not worry. I was told I would get a raise so one will happen soon.					
d. I would wonder if my supervisor was trying to take advantage of me.					

**Scenario 8.**

Imagine one afternoon you are home and your doorbell rings. You aren't expecting anyone, and you look through the peephole in your door. The person, who you don't recognize, is carrying pamphlets, a clipboard, and a box.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would wonder if the person is there to take advantage of me in some way.					
b. I would be certain that this is a solicitation that I did not want, and I would do something such as keep quiet and not even answer the door.					
c. I would open the door and invite the person inside my home.					
d. I would answer the door and ask questions to determine why the person is there.					

**Scenario 9.**

Imagine you have pulled off an interstate to stop for gas at a gas station. You are approached by a male asking for money. He tells you his car broke down, and he and his spouse are on their way to a family member's funeral.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would look to see if I have any money I could spare.					
b. I would be certain that this person is conning me, and I would do something such as call the police or quickly walk away from him.					
c. I would wonder if the person is lying to take advantage of me.					
d. I would ask him questions to try to determine if his story was accurate or what it might really be.					

**Scenario 10.**

Imagine you are using your computer for a search on a topic of interest. You soon notice that your computer is running slower than normal.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. I would be certain that there is something very wrong, and I would do something such as immediately shut the computer down without completing my search.					
b. I would worry that someone is trying to hack into my computer to cause me harm.					
c. I would keep working on the search – it's likely nothing to be concerned about.					
d. I would try to think of reasons the computer could be running slow.					

**Scenario 11.**

Imagine you are at a convenience store and you need to pay your bill. The charge for your items is \$20.57, and you give \$30 in cash to the attendant. He gives you 43 cents, a \$5 bill, and a \$1 bill in return.	Not at all accurate	Minimally accurate	Somewhat accurate	Accurate	Very accurate
a. After counting my change, I would wonder if the error was made on purpose					
b. I would not count my change, and I would put it away without a second thought.					
c. After counting my change, I would think about possible reasons that I did not get what I expected to get.					
d. Before even looking at my change, I would be certain that it was wrong and that the attendant is like all cashiers – who always try to short-change customers – and I would immediately count my change in front of him.					

## Appendix C: Personality Questionnaire

Purpose: The purpose of this questionnaire is to gain insights into your general inclination towards the others and/or the actions of others.

Instructions: Read each of the following statements carefully and circle the number that best describes how much you agree or disagree with each statement using the 7-point scale provided below.

1	2	3	4	5	6	7
Strongly Disagree	Disagree	Slightly Disagree	Neutral	Slightly Agree	Agree	Strongly Agree

1. Most experts tell the truth about the limits of their knowledge.

1                      2                      3                      4                      5                      6                      7

2. Most people can be counted on to do what they say they will do.

1                      2                      3                      4                      5                      6                      7

3. Most adults are competent at their jobs.

1                      2                      3                      4                      5                      6                      7

4. Most salespeople are honest in describing their products.

1                      2                      3                      4                      5                      6                      7

5. Most people answer public opinion polls honestly.

1                      2                      3                      4                      5                      6                      7

6. These days, you must be alert, or someone is likely to take advantage of you.

1                      2                      3                      4                      5                      6                      7

7. One should be very cautious with strangers.

1                      2                      3                      4                      5                      6                      7

8. Most repair people will not overcharge people who are ignorant of their specialty

1                      2                      3                      4                      5                      6                      7



## Appendix D: Mission Scenario Questionnaire

Purpose: The purpose of this questionnaire is to gain insights into your perception of the described mission scenarios.

Instructions: For the following scenarios, please read the description and select the response which most closely aligns with the action(s) you would take.

1. Scenario: After signing into your work computer one morning, you observe an unexpected software installation. Not thinking much of the software, you begin to read your work emails when you notice that the software is attempting to access your computer's microphone and webcam.

Based on your initial assessment, select the best response from the list below:

- A. Continue working on your computer, paying extra attention to any irregular activity that may further indicate the presence of a hacker.
- B. Immediately power down your computer, the hacker cannot persist if the processor is not turned on.
- C. Leave your computer running and immediately report the incident to your office's security manager.

2. Scenario: You are an RPA pilot conducting a mission that has been extended due to unforeseen circumstances. With extremely low fuel levels, you now have to stop at a nearby base to refuel in order to conduct the extended mission. However, the shortest route to the base is programmed to fly through Iranian airspace.

Based on your initial assessment, select the best response from the list below:

- A. Divert the drone to land in an unsecure airfield in Afghanistan where US forces are present, but there may be unknown threats
- B. Fly the drone on the shortest route possible, which happens to be contested airspace which Iran has recently claimed as their own.
- C. Crash land the drone in the Arabian gulf and send US Naval troops to recover the aircraft (ensure destruction). This will result in a loss of the US asset would prevent it from falling into the hands of the enemy.

3. Scenario: Imagine you are a cyber operator monitoring the communications and weapons systems on an F-22 mission. Shortly after refueling at a friendly base, you observe traffic on the aircraft's mission systems that deviate substantially from its known baseline. This indicates the potential for onboard systems being compromised.

Based on your initial assessment, select the best response from the list below:

- A. Shut down communication with the aircraft. This will ensure that adversary forces can no longer listen to information regarding the mission, however, it will also cut coordination with the F-22.

- B. Continue to monitor the network traffic and instruct the F-22 to continue its mission as planned.
- C. Abort the mission and instruct the F-22 to land at the nearest base.

4. Scenario: You are the ranking officer on a logistics convoy in a combat zone. You have received intelligence from one of the locals working on the base that ISIS has intercepted communications (mission details) regarding the convoy from one of the troops' cell phones.

Based on your initial assessment, select the best response from the list below:

- A. Continue on predetermined patrol (mission as planned) with increased security along route.
- B. Ensure all airmen turn off their cellphones. Reschedule the mission for a different time along a different route, which will allow for 80% completion of the original mission
- C. Cancel the mission altogether.

5. Scenario: You are an offensive Cyber Operator and are aiming to investigate the Chinese militarization of the South China Sea. You successfully infiltrate a Chinese Surface-to-Air Missile (SAM) System and realize they are currently targeting an allied vessel in the region.

Based on your initial assessment, select the best response from the list below:

- A. You continue to monitor the Chinese activity, collecting intelligence while remaining undercover in the system.
- B. You attempt to disable the system. This will protect the allied vessel from a potential attack but will also reveal your presence to the Chinese in the intelligence system.
- C. You stop monitoring the intelligence systems and inform the allied vessel of the potential threat.

6. Scenario: You are a Cyber Operations Officer supporting an intelligence gathering mission targeting a Chinese Nuclear Enrichment Facility. While attempting to infiltrate potentially useful intelligence, you realize that your network traffic has been identified by Chinese cyber security protocols.

Based on your initial assessment, select the best response from the list below:

- A. Do your best to infiltrate as much information as possible before enemy forces eliminate you from the network.
- B. Immediately stop transmitting. Passively monitor the network traffic until you believe it is safe to transmit the remaining intelligence.
- C. Stop transmitting and remove any attributable data so that your exploitation methods could be preserved for future missions.

## Bibliography

- Bigley, G.A., Pearce, J.L., 1998. Straining for shared meaning in organization science: problems of trust and distrust. *Academy of Management Review* 23 (3), 405–421.
- Bobko, P., Barelka, A. J., & Hirshfield, L. M. (2014). The construct of state-level suspicion: A model and research agenda for automated and information technology (IT) contexts. *Human Factors*, 56(3), 489–508. doi:10.1177/0018720813497052
- Bobko, P., Barelka, A. J., Hirshfield, L. M., & Lyons, J. B. (2014). Invited Article: The Construct of Suspicion and How It Can Benefit Theories and Models in Organizational Science. *Journal of Business and Psychology*, 29(3), 335–342. doi:10.1007/s10869-014-9360-y
- Botta, D., Werlinger, R., Gagne, A., Beznosov, K., Iverson, L., Fels, S., & Fisher, B. (2007). Towards Understanding IT Security Professionals and Their Tools. *N Proc. of the 3rd Symposium on Usable Privacy and Security: SOUPS '07*. 100-111
- Carretta, T. R. (2013). Predictive Validity of Pilot Selection Instruments for Remotely Piloted Aircraft Training Outcome. *Aviation, Space, and Environmental Medicine*, 84(1), 47–53. doi: 10.3357/ase.3441.2013
- Cohen, J. (1992). A Power Primer. *Psychological Bulletin*, 112(1), 155–159. <http://doi.org/10.1037/0033-2909.112.1.155>
- Deutsch, Morton. “Trust and Suspicion.” *Journal of Conflict Resolution*, vol. 2, no. 4, 1958, pp. 265–279., doi:10.1177/002200275800200401.
- Ebenbach, D. H., & Moore, C. F. (2000). Incomplete information, inferences, and individual differences: The case of environmental judgments. *Organizational Behavior and Human Decision Processes*, 81(1), 1–27. doi:10.1006/obhd.1999.2870
- Evans, K., & Reeder, F. (2010, November 15). A Human Capital Crisis in Cybersecurity. Retrieved from <https://www.csis.org/analysis/human-capital-crisis-cybersecurity>
- Falcone, Rino, et al. *Trust in Cyber-Societies: Integrating the Human and Artificial Perspectives*. Springer, 2001.
- Fein, S. (1996). Effects of suspicion on attributional thinking and the correspondence bias. *Journal of Personality and Social Psychology*, 70, 1164–1184.
- Full Scale. (2019, November 4). Talent Shortage of Software Developers. Retrieved from <https://fullscale.io/talent-shortage-software-developers/>.
- GAO. DOD training: U.S. Cyber Command and services should take actions to maintain a trained cyber mission force: report to the Committee on Armed Services, House of Representatives, DOD training: U.S. Cyber Command and services should take actions to maintain a trained cyber mission force: report to the Committee on Armed Services, House of Representatives (2019). Washington, D.C.: United States Government Accountability Office.

- Haney, J. M., & Lutters, W. G. (n.d.). Workshop on Security Information Workers, Symposium on Usable Privacy and Security (SOUPS) 2017. *Skills and Characteristics of Successful Cybersecurity*.
- Hambrusch, S. (2017). NAS Report Investigates the Growth of Computer Science Undergraduate Enrollments. *Computing Research News*, 29(10).
- Hilton, J., Fein, S., & Miller, D. (1993). Suspicion and dispositional inference. *Personality and Social Psychology Bulletin*, 19, 501–512.
- Hoff, K. A., & Bashir, M. (2015). Trust in Automation. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 57(3), 407–434. doi: 10.1177/0018720814547570
- Khazon, S., & Bowling, N. (2016). *Changes in State Suspicion Across Time: An Examination of Dynamic Effects* (Doctoral dissertation, Wright State University). CORE Scholar.
- Kim, R., & Levine, T. (2011). The effect of suspicion on deception detection accuracy: Optimal level or opposing effects? *Communication Reports*, 24, 51–62.
- Lange, K. (2018, May 4). Cybercom Becomes DoD's 10th Unified Combatant Command. Retrieved from <http://www.dodlive.mil/2018/05/03/cybercom-to-become-dods-10th-unified-combatant-command/>
- Lee, J. D., & See, K. A. (2004). Trust in Automation: Designing for Appropriate Reliance. *Human Factors*, 46(1), 50–80. doi:10.1518/hfes.46.1.50.30392
- Leigh, Jennifer, and Brig. Gen. DeAnna Burt. “USAF Improves Space Training to Address Space Threat Despite Ongoing Space Force Debate.” *Air Force Magazine*, 2 Nov. 2018.
- Losey, S. (2018, August 3). Now's your shot: The number of retraining slots in the Air Force just exploded. Retrieved from <https://www.airforcetimes.com/news/your-air-force/2018/08/03/nows-your-shot-the-number-of-retraining-slots-in-the-air-force-just-exploded/>
- Lyons, J. B., Stokes, C. K., Eschleman, K. J., Alarcon, G. M., & Barelka, A. J. (2011). Trustworthiness and its suspicion: An evaluation of the nomological network. *Human Factors*, 53(3), 219–229. doi:10.1177/0018720811406726
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An Integrative Model of Organizational Trust. *Academy of Management Review*, 20(3), 709–734.
- Mayer, J., & Mussweiler, T. (2011). Suspicious spirits, flexible minds: When distrust enhances creativity. *Journal of Personality and Social Psychology*, 101(6), 1262–1277. <http://doi.org/10.1037/a0024407>
- Mcknight, D., Choudhury, V., & Kacmar, C. (2002). The impact of initial customer trust on intentions to transact with web site: A trust building model. *Journal of Strategic Information Systems*, 11, 297–323.
- Pervin, L. A., & John, O. P. (1999). *Handbook of personality Theory and research*. New York: The Guilford Press.

- Pomerleau, M. (2018, August 08). Here are the cyber staffing issues facing the Defense Department. Retrieved from [https://www.fifthdomain.com/dod/cybercom/2018/08/03/can-cyber-command-overcome-its-staffing-shortage/?fbclid=IwAR3Cd1\\_5CH47IbTTdcPZ5f-0VeGGD6HhLBcgalGNdqZdEHcDX-bcaFDqdPg](https://www.fifthdomain.com/dod/cybercom/2018/08/03/can-cyber-command-overcome-its-staffing-shortage/?fbclid=IwAR3Cd1_5CH47IbTTdcPZ5f-0VeGGD6HhLBcgalGNdqZdEHcDX-bcaFDqdPg)
- Ridings, C. M., Gefen, D., & Arinze, B. (2002). Some antecedents and effects of trust in virtual communities. *Journal of Strategic Information Systems*, 11(3/4), 271.
- Smit, A. S., Eling, P. A. T. M., & Coenen, A. M. L. (2004). Mental effort causes vigilance decrease due to resource depletion. *Acta Psychologica*, 115(1), 35–42. doi: 10.1016/j.actpsy.2003.11.001
- Somers, D., & Moody, J. (2019, September 11). 10 College Majors With the Highest Starting Salaries. Retrieved from <https://www.usnews.com/education/best-colleges/slideshows/10-college-majors-with-the-highest-starting-salaries>.
- “Space Systems Operations.” *U.S. Air Force - Career Detail*, United States Air Force Recruiting Service and the Department of the Air Force, [www.airforce.com/careers/detail/space-systems-operations](http://www.airforce.com/careers/detail/space-systems-operations).
- Trust in Automation: Integrating Empirical Evidence on Factors That Influence Trust. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 57(3), 407–434. <https://doi.org/10.1177/0018720814547570>
- United States., Department of Defense, Joint Chiefs of Staff. (n.d.). *Cyberspace Operations*.
- U.S. Air Force. “Pilot.” *U.S. Air Force - Career Detail*, United States Air Force Recruiting Service and the Department of the Air Force, [careers.airforce.com/careers/detail/pilot](http://careers.airforce.com/careers/detail/pilot).
- Wee, C., Bashir, M., Lambert, A., & Guo, B. (2016). Understanding the Personality Characteristics of Cybersecurity Competition Participants to Improve the Effectiveness of Competitions as Recruitment Tools. *Advances in Intelligent Systems and Computing Advances in Human Factors in Cybersecurity*, 111-121. doi:10.1007/978-3-319-41932-9\_10

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. <b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b>					
1. REPORT DATE (DD-MM-YYYY) 03/26/2020		2. REPORT TYPE Master's Thesis		3. DATES COVERED (From - To) Sept 2018 - March 2020	
4. TITLE AND SUBTITLE Recognizing Potential Cyberspace Warriors Through the use of Suspicion Propensity Index				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Strang, Meghan G, 2LT				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Institute of Technology Graduate School of Engineering and Management (AFIT/EN) 2950 Hobson Way Wright-Patterson AFB OH 45433-7765				8. PERFORMING ORGANIZATION REPORT NUMBER AFIT-ENV-20-M-244	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) Kyle J. Gearan, MSgt Manager – Cyber ISR Capabilities 1700 Air Force, Pentagon Washington, DC 20330-1700				10. SPONSOR/MONITOR'S ACRONYM(S) A2/6CX/A3CZ	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Distribution Statement A. Approved for public release; Distribution unlimited.					
13. SUPPLEMENTARY NOTES This work is declared a work of the U.S. Government and is not subject to copyright protection in the United States.					
14. ABSTRACT The Suspicion Propensity Index and Mayer's trust questionnaire are used along with a cyber-mission performance questionnaire to investigate different attributes that may indicate high performance in the cyber career field. One hundred twenty two total individuals participated in this research, 57 from the cyber career field and 65 from other various careers. Evidence suggests that suspicion is highly correlated with cyber mission performance. Years of experience displays a more prominent role in suspicion of cyberspace individuals compared to their non-cyber counterparts. Trust is not significantly correlated with overall cyber mission performance.					
15. SUBJECT TERMS Suspicion, trust, cyber, performance					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Michael E. Miller, AFIT/ENV
U	U	U	UU	76	19b. TELEPHONE NUMBER (Include area code) (937) 255-3636x4651 michael.miller@afit.edu