9-3-2019

Trust and Suspicion as a Function of Cyber Security in Human Machine Team (HMT) of Unmanned Systems

Dhaher M. Alshammari

Trust and Suspicion as a Function of Cyber Security in Human Machine Team (HMT) of Unmanned Systems

THESIS

Dhaher M. Alshammari, 1st Lt, RSAF

AFIT-ENV-MS-19-S-051

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

APPPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITEDAPPPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITEDAPPPROVED 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.

Trust and Suspicion as a Function of Cyber Security in Human Machine Team (HMT) of Unmanned Systems

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Engineering Management

Dhaher M. Alshammari, BS

1st LT, RSAF1st LT, RSAF1st LT, RSAF

AUGUST 2019

Trust and Suspicion as a Function of Cyber Security in Human Machine Team (HMT) of Unmanned Systems

THESIS

Dhaher M. Alshammari, BS

1st LT, RSAF

Committee Membership:

Dr. John J. Elshaw
Chair

Dr. Alfred E. Thal, Jr.
Member

Dr. Brent T. Langhals
Member

Abstract

The research focuses on cyber-attacks on cyber-physical systems of the unmanned vehicles that are characteristically used in the military, particularly the Air Force. Unmanned systems are exposed to various risks as the capacity of cyber attackers continue to expand, raising the need for speedy and immediate responses. The advances in military technologies form the basis of the research that explores the challenges faced in the timely detection and response to cyber-attacks. The purpose of the research is to study the connections between operator suspicion and the detection and response to cyber-attacks alongside the identification of theory of suspicion as the theoretical framework. The paper further presents the experiment used and the interview questions that offer the basis for the recommendations and importance of the research while answering the research questions. The conclusion from the literature review, interview, and experiment indicates the need for training among operators in the Air Force to reinforce their capacity in the detection and response to cyber-attacks and other adverse events that could compromise the execution of the mission established for unmanned systems. The research offers recommendations that can be implemented by the Royal Saudi Air Force (RSAF) in enhancing the security measures of unmanned systems.

To my God, with whom all things are possible.

To my mother

To my father

To my brother

To my sisters

To my country

For their unwavering support.

Acknowledgements

I would like to express my sincere appreciation to my faculty advisor, Dr. John J. Elshaw for his guidance and support throughout the course of this thesis effort. I would also like to thank my committee members Dr. Alfred E. Thal, Jr. and Dr. Brent T. Langhals who supported me and provided their expertise during every step in the research process. The success of this research effort was made possible by the work and dedication of each of the members of the research team. I would also like to thank Maj. Loay Almannai. from Royal Bahrain Air Force for both the support and encouragement provided to me in this endeavor.

Table of Contents

List of Figures

List of Tables

Trust and Suspicion as a Function of Cyber Security in Human Machine Team (HMT) of Unmanned Systems

I. Introduction

1.1 Background

Cyber-attacks on the cyber-physical systems (CPS) of unmanned vehicles are attracting significant research interest as emergent threats whose catastrophic impacts have significant ramifications on security systems. Unmanned Aerial Vehicles (UAVs) are being used more and more, particularly by the Saudi military and U.S. military, increasing their investments in research and production by more than one hundred percent. The uses for UAVs during missions include transportation, armed attacks, reconnaissance, and border surveillance (Wang, Yan & Zheng, 2018). The unmanned systems are associated with the provision of reliable, autonomous, automated, and timely services targeted at the improvement of national security. The unmanned systems are expected to collect and process data that could be important to national security. The importance of the systems has contributed to the widening of research regarding possible cyber-attacks that could compromise the integrity of the information and task that unmanned systems are expected to accomplish.

1.2 Motivation

The applications of unmanned systems largely increased since they can be used in gas detection, rescue missions, and monitoring hazardous surroundings. The systems also enable experts to capture videos and images affected by natural disasters such as floods, hurricanes, and earthquakes (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). Cyber-attacks are against data integrity and aimed at modifying legitimate data by introducing falsified information onto the sensors. Cyber-attacks refer to developing threats, resulting in interest by martial forces. UAVs enable malicious individuals to exploit susceptibility from a distance and obtain information that cannot be remotely accessed. Despite the advantages of unmanned systems, the devices encounter various risks, especially cyber hacking (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). Cyber hackers complete tasks by introducing a raspberry computer, a battery, and wireless transmitters into the unmanned system that facilitates the access into the systems via WIFI-signals.

However, experts must recognize the infected systems by applying an algorithm based on some features such as the type and the number of collected data that will be important in the training procedure. Another threat in distorting the availability of network is Denial of Service (DoS), which agitate the protocol routine operations (Wang, Yan & Zheng, 2018). With an increase in cyber-attacks, the government ought to develop technology to analyze and comprehend the preventive measures against threats. Additionally, it is essential to identify the risks against technological advancements in unmanned systems, for example, the motor, battery, propellers, WI-FI receivers, and Global Positioning Systems (GPS) among others (Kwon, Liu & Hwang, 2014). Measures should be implemented on identifying the methods used by hackers to access the unmanned systems.

The research framework places emphasis on the intervention of operations at the right moment based on suspicious activities that could threaten the integrity of CPS' (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). Nonetheless, research indicates that operators in the military setting are trained to trust the systems as opposed to creating suspicions on their operations (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). The suspicion theory is an important framework that can be applied to explore the means through which operators detect and create response mechanisms to cyber-attacks that target unmanned systems of ground and aerial vehicles (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). UAV systems and unmanned ground vehicle (UGV) systems are both prone to various cyber-attacks that could compromise the integrity of the mission they are designed to complete (Kwon, Liu & Hwang, 2014).

The majority of the cyber-attacks are not instantaneous but are characterized as time and resource-intensive activities orchestrated by humans and unfold at human speeds. The elements of cyber-attacks contribute to the preparation and introduction of safeguards promptly based on the preparedness and suspicion of operators (Wang, Yan & Zheng, 2018). As a suitable example, the Iranian cyber capabilities were linked to the manipulation and grounding of the Central Intelligence Agency (CIA) operated RQ-170 Sentinel drone conducting operations at the Iranian border (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). The example magnifies the effects that could be linked to cyber-attacks on sensitive unmanned systems used for security purpose and the gathering of intelligence. It further highlights the challenges of unprepared operators who require high suspicion levels to either avert possible cyber-attacks or minimize the leakage of sensitive information in case the ground or aerial vehicle is compromised. The research regarding the human component (operator) in cyber-attack detection and response remains scarce and continues being developed to ensure operator suspicions can generate the needed response to possible cyber-attacks against CPS (Gay, Horowitz, Elshaw, Bobko & Kim, 2019).

The Suspicion theory, as postulated by Bobko offers the theoretical model applied in the research to understand how operators can detect and respond to cyber-attacks on unmanned systems (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). The theoretical definition indicates the simultaneous state of uncertainty, perceived malintent, and cognitive activity regarding the underlying information generated electronically and is collated, analyzed, sent, or implemented by an external agent (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). According to the framework, it is evident that the state of suspicion among operators is linked to the capacity of the Human-Machine Team (HMT) in the response to cyber-attacks. The underlying challenge is linked to the design of high-performance HMT in understanding the interactions between machines and humans in the working context to minimize the cases of attacks against unmanned aerial and ground vehicle systems.

The literature contributes to the primary goal of the research that shall seek to establish the influence of operator suspicion in the detection and response to cyber-attacks against unmanned aerial and ground vehicle systems in the context of the HMT. The research will apply suspicion theory as the guiding framework in the investigation and understanding of the interaction between humans (operators) and machines in averting cyber-attacks on the unmanned vehicles. The use of different scenarios will be insightful in understanding the importance of operator suspicion in the determination of the response to possible and ongoing attacks. The results from the study will be important in guiding military operations and filling the existing gap among military operators who have the capacity to trust and not become suspicious.

1.3 Problem Definition

Cyber-Physical Systems (CPS) have often experienced cyber-attacks that have drawn attention to how such utilities as unmanned vehicles can be more secured. Specific attention has been paid to their human operators, which is the case mostly in the US military where unmanned aerial vehicles (UAVs) or drones have been increasingly used for missions (Wang, Yan & Zheng, 2018). These unmanned systems can be compromised as they are remotely operated and use sensors whose signals can be interfered with electronically to give falsified information to surveillance agencies such as the military. Operator suspicion presents a scenario in which the threat of cyber hacking of the UAVs is detected (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). Through such systems as DoS (Denial of Service) and GPS (Global Positioning System), operators can identify security risks and try to mitigate against them (Wang, Yan & Zheng, 2018; Kwon, Liu & Hwang, 2014). This research problem emphasizes on such timely intervention to address suspicious activities noted by operators on these UAVs, although training of military personnel is more towards trust than suspicion of such systems (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). The suspicion theory according to Gay, Horowitz, Elshaw, Bobko and Kim (2017) will be used for the theoretical grounding to gain an understanding of the manner in which operators can detect, as well as respond to cyber-attacks on these UAVs, even as the cognitive load that they face is explored to establish the impact on their perceptions and performance on the job as elucidated by Paul and Dykstra (2017).

1.4 Research Questions

The current study is based on research questions that focus on the critical analysis of operator suspicion and trust in the cybersecurity of unmanned systems, with the final set of questions explored a pertinent suspicion dimension and how it affects the perceptions of operators and their work performance.

The focus research questions (denoted as FRQ) that I focused on were as follows:

- **FRQ1:** What is the significance of operator suspicion and the detection and response to cyber-attacks on unmanned vehicles?

- **FRQ2:** How do trust and suspicion relate to each other? Are they at opposite ends of the same construct, or do they act independently of each other?

The other questions (denoted as SQ – Supplemental Question) that supplemented the FRQs went further to explore dimensions of suspicion theory with focus on an aspect that is pertinent to operators of the security systems.

- **SQ1:** How do the dimensions of suspicion (uncertainty, malintent, cognitive activation) relate to operator performance? Which dimensions have the largest impact on operator performance?

- **SQ2:** How do the dimensions of suspicion impact cognitive workload? How is cognitive workload affected by suspicion, trust, and personality?

1.5 Hypotheses

Related to the focus research questions are the following hypotheses or focus research hypotheses (FRH) even as majorly based on Gay, Horowitz, Elshaw, Bobko and Kim (2017), as well as Gay, Horowitz, Elshaw, Bobko and Kim (2019)

- **FRH .1.1:** Operator suspicion is significant in detection of cyber-attacks on UAVs.

- **FRH .1.2:** Detection is positively linked to the speediness of response to the suspicious activity.

- **FRH.2.1:** Trust and suspicion are related.

- **FRH.2.2:** They are inversely related as opposite ends of the same construct.

Related to the supplemental questions were the following hypotheses, marked as SH – supplemental hypothesis addressing the aspect of cognitive load in suspicion theory as per Gay, Horowitz, Elshaw, Bobko and Kim (2017), as well as Paul & Dykstra (2017).

- **SH.1.1:** The three dimensions of suspicion negatively affect operator performance.

- **SH.1.2:** Operator performance is largely impacted by cognitive load.
- **SH.2.1:** Cognitive workload is increased by having to differentiate suspicion and trust.
- **SH.2.2:** Personality of the operator towards being highly suspicious or highly trusting positively increase cognitive workload.

1.6 Organization of the Dissertation

The dissertation will be organized and structured under various chapters as follows; Chapter 2: Literature review on cyber-attacks, suspicion theory, and the application. Chapter 3: Methodology that identifies the research design, provides an interview with one of the students in AFIT from the system engineering department, and experimentation used in answering the research questions. Chapter 4: Results and Discussion outlining the results from the study, discussion based on the literature available on the topic, and the limitations of the research. Chapter 5: Conclusion that offers a summary, and the recommendation for future research.

II. Literature Review

2.1 Chapter Overview

This chapter offers a synthesis of existing literature discussing and detailing various issues, concepts, and definitions related to the subject of operator suspicion and detection as the response to cyber-attacks on unmanned systems. This chapter offers a refined review of the literature that relates to the study hypotheses and helps answer the research questions about suspicion theory.

2.2 Background

Security issues that face unmanned systems particularly the UAVs and UGVs have been at the center of the attention of industry and researchers. The interest in preserving the integrity of the security of the unmanned systems shows a link to the increase in the number of attacks that target the systems, including jamming communications, injecting wrong data, and disturbing network operations (Sedjelmaci, Senouci & Messous, 2016). Unmanned aerial and ground vehicles, or drones, are increasingly important and serve a range of functions including surveillance and combat missions. UAVs and UGVs carry and collect or communicate sensitive information for the attacks (Jamshidi, Jaimes Betancourt & Gomez, 2011). The United States Army, Navy, and Air Force rely heavily on UAVs and UGVs to complete dangerous and traditionally exhausting manned missions to make them more feasible (Kim, Wampler, Goppert, Hwang & Aldridge, 2012).

The use of unmanned systems which was largely relegated to surveillance and reconnaissance operations has shifted as the government now use the systems for offensive purposes and other missions. The Federal Aviation Administration (FAA) expects that more than

30,000 drones will be flying in the country by 2020 (Paganini, 2019). Usage of the vehicles contributes to research concerns regarding the security of the unmanned systems that could be hacked and controlled by attackers that operate in complex environments compromising the mission. The majority of the cyber-attacks are not instantaneous with the push of a button but rather are resource and time-intensive activities that are carried out by humans and unravel at human speeds (Paganini, 2019).

The time and resources required by the adversary have a direct correlation and proportion to the quality and level of defenses employed on the network. Notably, the importance of considering the human element associated with cyber-attacks on unmanned systems cannot be overstated based on the arguments regarding the nature and ways of perpetrating attacks (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). Human vulnerabilities pose some of the greatest risks that could lead to attacks enhancing the need for examining the topic of operator suspicion and detection (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). According to Hirshfield et al. (2015) the importance of examining human errors in the cyber domain cannot be overlooked. While the majority of the cyber-warfare related research has concentrated on the effects of cyber-attacks on the targeted computer systems, it is important to consider the role of human operators during cyber breaches (Hirshfield et al., 2015).

However, businesses must align response policy with an institution's values and responsibilities in handling an attack. For example, when Arabian-American Oil Company (ARAMCO) was hacked, as soon as the company was aware of the hacking event, the company's electronic systems were wholly isolated and stopped from the outside as an early precautionary measure taken with the start of the emergency damage that hit some sectors of its electronic network, which is suspected to be caused by the entry of a virus into a number of personal computers in the company without being able to hit the main components of the network. I know the example is not related to the Unmanned Aerial Vehicle (UAV) but they share a strong concept between them which is Operator suspension and detection toward the system that has been hacked while observing. Both examples will let me study more how Operator should be aware of situation.

2.3 Suspicion Theory

Failure and System errors that have been predicted by Operator may occur during system run so in this case, full mission capable and stability of the system are not guarantee. Cyber-attack does not have a specific time of occurrence so it may occur at any time. The operator must also believe that any attack may occur in times that are considered quiet, normal or what do you call a perfect day. Aramco example is the most significant proof of that, it was attacked where most of the IT employees are on leave. Therefore, Operator must always be caution of satiation awareness of the whole operation, and full readiness of reaction with speed for any strange event occurs like failure and errors in system or system of system such as Unmanned Aerial Vehicle (UAV) and Ground Control Station (GCS).

The major emphasis regarding operator suspicion and threat detection concerns the need for interventions at the appropriate time based on the identification of suspicious activities that could pose threats to the integrity of Cyber-Physical Systems (CPS). However, the operators in the military, for example, receive training on the need for trusting the system as opposed to the necessity of creating suspicions that could be used to deal with possible threats that might affect the system (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). Therefore, research highlights the importance of anchoring operator suspicion on training, particularly among military operators based on Suspicion Theory as the main and guiding theoretical framework (Gay, Horowitz, Elshaw, Bobko & Kim, 2017).

Suspicion Theory, as discussed on the security of unmanned systems, addresses the need for operators to be keen and alert to possible attacks as a means of ensuring they can detect and create the appropriate responses to cyber-attacks. Further, suspicion theory is premised on the majority of the attacks being time and resource-intensive; therefore, the emphasis on need for suspicion and training for detection of suspicious activities that could threaten the integrity of the system could lead to improved operator detection and aversion of threats (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). The available literature on suspicion theory indicates the need for training as the anchor to improve responses and measures against impending attacks on the unmanned systems that could empower the activities of hackers (Gay, Horowitz, Elshaw, Bobko & Kim, 2017).

2.4 Constructs and Application of Suspicion Theory

Indicators of an attack include anti-malware programs, system administrators reporting indications of a breach, and suspicious activity with operating services and different users. Upon detection of an attack, IT experts must control the damage by disconnecting system access for computers infected by malware and setting up security measures to eliminate network vulnerability (Manesh & Kaabouch, 2019). The application of suspicion theory illustrates a way to assist in comprehending operator performance in circumstances that entail malicious objectives such as a cyber-attack (Manesh & Kaabouch, 2019). A study by Manesh & Kaabouch (2019) was conducted to apply suspicion theory in surveying how operators identify and respond to cyber-attacks against unmannered systems. The operator suspicion ought to be controlled for the human-machine to achieve better results based on detecting cyber-attacks, and develop appropriate responses when the unmannered systems are exposed to attacks (Manesh & Kaabouch, 2019).For example, Iran provides a case of the challenges possibly associated with cyber-attacks as its capabilities were linked to the grounding of RQ-170 Sentinel drone operated by the Central Intelligence Agency (CIA) and commissioned to conduct activities at the Iranian border for security purposes (Gay, Horowitz, Elshaw, Bobko & Kim, 2019). As part of the example, it is important to note that unmanned systems could have great impacts on security if they are manipulated and land on the wrong hands. Notably, the leakage of sensitive information or diversion of the unmanned system could be used to the advantage of cyber attackers. However, research on the human aspects of the operators related to cyber-attack detection remains insufficient but continues to be the center of attention with suspicion theory being developed as the leading theoretical component to deal with the attacks on unmanned systems (Gay, Horowitz, Elshaw, Bobko & Kim, 2019).

The theoretical framework was advanced by Bobko and serves as the tool for understanding the means through which operators can facilitate the detection and response to cases of cyber-attacks on the unmanned systems used for different operations (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). The framework indicates the uncertainty associated with cyber-attacks and the need for vigilance as the solution to impending attacks stopped by operators through the collection, analysis, and enforcement of barriers against intrusion (Gay, Horowitz, Elshaw, Bobko & Kim, 2017). The framework further indicates the state of suspicion as being the inherent capacity of the Human-Machine Team (HMT) that facilitates the response to cyber-attacks. Hence, it is important to consider the design of high-performance HMT as the means of understanding the connection between humans and machines (unmanned systems) as the means of minimizing the risks associated with cyber-attacks.

Both empirical and conceptual research, using quantitative and qualitative methods, examine the role of operator suspicion in detecting and responding to cyber-attacks on unmanned systems such as is the case with drones. These have provided theoretical and empirical/experimental evidence on the workings of suspicion theory in informing human operators' response to cyber threats. Suspicion theory itself works as a good source point from which the relationships in the model can be explained since it links the cues to the filters, and ultimately the immediate derivatives and outcomes.

2.5 Human Factors and Suspicion are related to the Effects of Cyberattacks

Human-level factors play different roles when attacks are perpetrated leading to the need for exploring suspicion and detection as the means of averting impending attacks. Cyber security is one of the leading and important issues associated with unmanned systems, particularly aerial ones whose functions are heavily dependent on the onboard automation and intervehicle communications (Kwon, Liu & Hwang, 2014). The Unmanned Aerial Vehicles are operated remotely or in other incidences flown using automated piloting and face the same vulnerabilities that unmanned systems are exposed to (Kwon, Liu & Hwang, 2014). Cyber-attacks that target Cyber-Physical Systems (CPS) and unmanned vehicles are emergent threats that carry with them catastrophic risks and impacts that could affect the activities of military agencies as the major users of the unmanned vehicles (Gay, Horowitz, Elshaw, Bobko & Kim, 2017).

Cyber hackers may turn to information breach by generating software to destroy a system's program. Infringement on data might greatly affect the security of a system when the attackers have sufficient data to carry out deceptive activities. Examples of cyber-attacks on unmannered aerial systems include:

- Jamming is an unwanted signal that leads to the blurring of real information or the fallacy or deception or concealment of such information. The source of such interference may be natural due to electromagnetic phenomena such as multi-track interference or industrial interference planned by the enemy.
- Message deletion where the hacker detects the messages sent from the operator to the Unmanned Aerial Vehicle (UAV) and deletes them before reaching the UAV, or the hacker prevents the signals and messages sent from the UAV to the operator in the ground.
- GPS spoofing is considered an attack where a radio transmitter is used close to the target by applying signals to interfere with the GPS signals, which means that they can be intercepted and controlled.
- Fault injection by intruder.

The attacks may result in collisions of systems providing aircraft controllers falsified information. However, the government might respond to criminal activities by making certain experts follow the best criteria when setting up passwords for example. Further, frequent checkups of passwords may prevent the cyber attackers from access into the unmanned systems. IT experts ought to develop a plan that entails team members who will be involved in communication and implementing tasks to be undertaken in responding to cyber-attacks (Jamshidi, Jaimes Betancourt & Gomez, 2011). Further, the plan ought to be specific to individuals who could cover the operations in the event the assigned member is unavailable. Every person on the team must bring an exclusive institutional perspective, which will be essential in addressing the consequences of cyber-attacks.

Identifying cyber-attack is not easy at any jobs during observing operation. Training Operators of situation awareness with a perfect alert notification can be one of the solution to detect early clue in any security job. However, automated alarms are essential in recognizing intrusion into the systems and the source of the infringement (Jamshidi, Jaimes Betancourt & Gomez, 2011). Nevertheless, experts have to recognize the infected systems by applying an algorithm based on features such as the type and the number of collected data that will be important in training procedure. Another threat in distorting the availability of network is Denial of Service, which agitate the protocol routine operations. With an increase in cases of cyber-attacks, the government ought to develop technology in order to analyze and comprehend the preventive measures against threats. Additionally, it is essential to identify the risks against technological advancements in unmanned systems, for example, motor, battery, propellers, WI-FI receivers, and the Global Positioning Systems (GPS) amongst others (Ji, Niu & Shen, 2016). Measures ought to be implemented on identifying the methods used by hackers to access the unmanned systems and setting up the appropriate responses to cyber-attacks (Ji, Niu & Shen, 2016). Administration's response to cyber-attacks may escalate an incident, thus it is important for the management to identify procedures that are less costly, time efficient, as well as events that protect an organization's reputation.

Another response to cyber-attacks entails involvement of government in the investigation team. Further, an organization must align response attempts with security management and IT initiatives. Cyber security crews generate and implement methods of identifying, supervising, and responding to a cyber-crisis (Manesh & Kaabouch, 2019). In case of a cyber-attack, an investigation team must recognize grounds for breach and methods of containing the infringement.

Another significant way to respond to attacks involves the use of an intrusion detection system, which examines system attacks on unmanned aerials. Organizations must develop strategies to prevent and respond to cyber-attacks by implementing the best cyber security. Another response to cyber-attacks is comprehending the reason behind the infringement and focus attention on attacker's motives. On suspicion of a planned cyber-attack, an organization must establish recovery plans for all procedures and provide maximum support to existing technology (Moga, Boscoianu, Ungureanu, Sandu & Boboc, 2016). Companies with formulated cyber threat strategy where each member is familiar with their responsibilities, have increased chances of rising back after an attack.

As highlighted, unmanned vehicles are used for various purposes and missions that include border surveillance, reconnaissance, and armed attacks. The systems are effective as they reduce the overreliance on physical deployment of service personnel in areas of conflict or other parts of the globe that could require monitoring. The systems provide an array of information and contribute invariably to the provision of autonomous, timely, automated, and reliable services that contribute towards the improvement of national security (Wang, Yan & Zheng, 2018). Some security measures and tools exist including intrusion detection systems that are applied to avert possible attacks on the machines. However, the use of security tools does not deal with the threat from the human perspective that could be addressed by considering the human element as the weakest link in a system (Fan, Lwakatare & Rong, 2017).

2.6 State Suspicion Model

The necessity of a conceptual framework cannot be overstated with the target of IT suspicion being covered in a three-stage process model that indicates the state-level of suspicion. As demonstrated in Figure 1 below, state suspicion is understood based on multiple phases that recognize the application of cognitive activity, uncertainty, and perceived malintent that facilitates the minimization of the risks associated with cyber-attacks (Bobko, Barelka & Hirshfield, 2013).

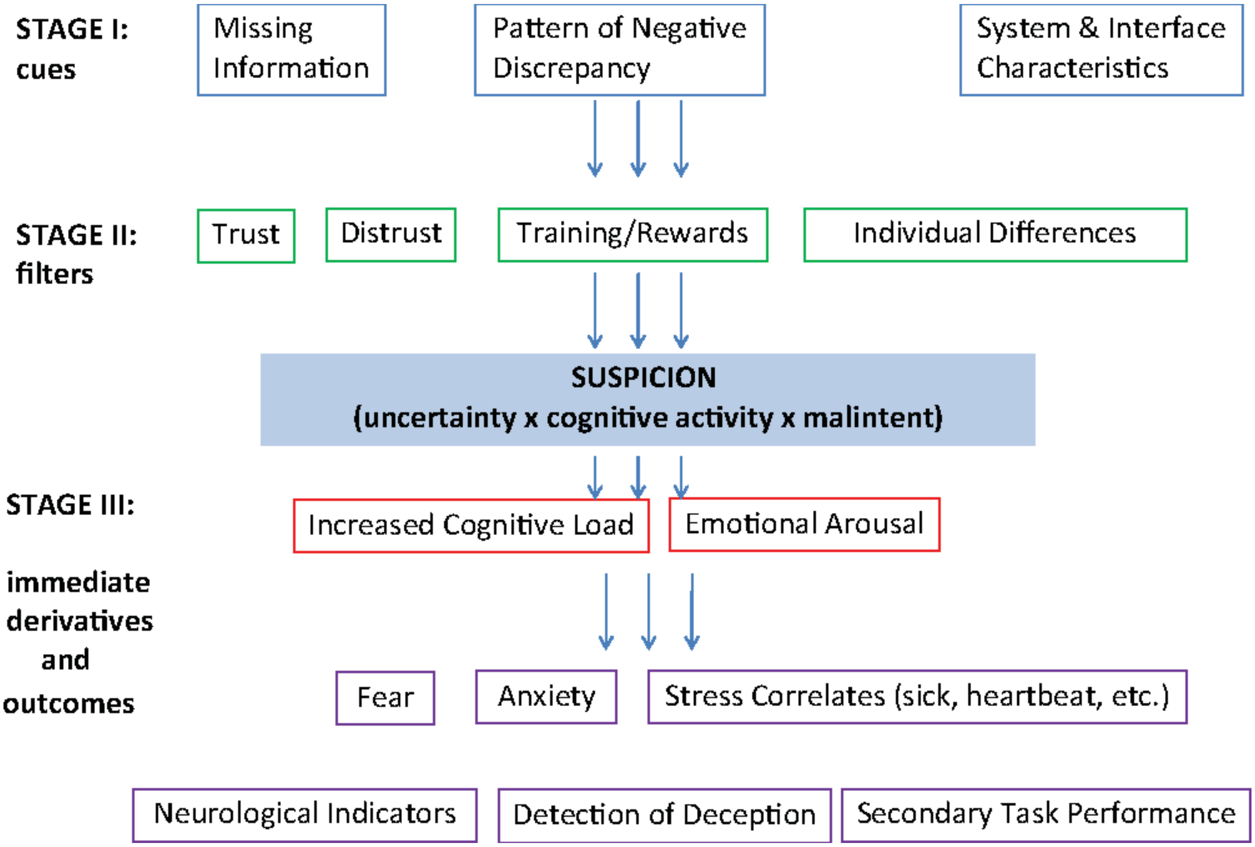


Figure 1: State-Level IT Suspicion (Bobko, Barelka & Hirshfield, 2013)

PHASE I: Cues that exist in the Environment

The three dimensions of suspicion are prevalent in the literature, although not explicitly mentioned, they are alluded to in the studies touching on operator suspicion in the detection of cyber threats in unmanned systems. For example, Clarke (2014) establishes some of the cues from the suspicion model regarding patterns of negative discrepancy when civilian drones are increasingly being used for malicious purposes and even enemy surveillance, which defeats their original purpose and raises suspicion among vigilant cybersecurity operators (Bobko, Barelka & Hirshfield, 2013). The variables of human behavior and activity characteristics in cyberspace have consistently shown up where operator suspicion has been mentioned, even as studies explore the human interface in cybersecurity operations. The cues include the pattern of negative discrepancies, system and interface characteristics, and missing information that deals with trust in IT systems.

PHASE II: Filters/ Individual Difference Determinants

Individual differences are associated as being critical in the increase or inhibition of state-level suspicion. For example, when a user displays trust in automation and IT services, there is a decreased chance of suspicion. When there is a lack of trust, it enhances the potential for suspicion contributing to the detection of possible cyber-attacks (Bobko, Barelka & Hirshfield, 2013). Moreover, the filters of training and rewards have been mentioned in studies, even as they link these to the immediate derivatives and outcomes of increased cognitive loads for human operators of cybersecurity. Despite growing efforts to foster an understanding of the intersection between humans and the cyberspace, there have been pertinent challenges in cybersecurity research. The presumption of the inscrutability of cyber technologies has created a sense of resignation, almost suggesting that cyber danger is beyond the ability of scholars to understand (Kello, 2013). In the third dimension, the cognitive load increment stands out, which is why most studies seem to refer to cognitive modeling as a way of addressing the multi-disciplinary cybersecurity challenges highlighted in human and computational sciences.

Phase III: Increased Cognitive Workload and How That Affects Perceptions and Performance on the Job

The human factor is very critical to the performance of any job and for the success of any operational activity. Since human beings use their mental capacities and are mandated to employ critical thinking in their different areas of work, they often bear a cognitive workload, which has the potential of affecting their perceptions and performances on the job. According to Paul and Dykstra (2017), little work or research on the human factor on cyber operations has been carried out despite being abundant in other mission-critical systems such as air traffic control, as well as cyber operations. Cybersecurity operations are regarded as a mission-critical service in the securing of organizations, companies, and even countries while ensuring business continuity. Evolving technology, coupled with threats to the network has increasingly made cybersecurity operations high-value, difficult, and quite complex (Paul & Dykstra, 2017). Similar to any other system, the complexity of tasks in the resultant high-risk environment is bound to take a toll on the human operators, often leading to judgment errors, burnout, and decreased performance. According to a comprehensive study of tactical cyber operations at the National Security Agency (NSA), operator fatigue, frustration, as well as cognitive workload increase significantly over the course of an operation inducing larger error margins and risk of attack (Paul & Dykstra, 2017).

The cybersecurity environment is one that poses considerable high risks in operation with failure or success, often affecting the mission and reputation of service providers adversely or positively. Paul and Dykstra (2017) assert that despite the heavy focus of cybersecurity operations' research and development on technology for the achievement of more secure enterprises, human experts are deemed as playing the most crucial role in deploying, configuring, monitoring, and operating the networks. The NSA often engages in the recruitment and hiring of computer network operators charged with defending US military networks and exploiting foreign adversaries' networks (Paul & Dykstra, 2017). These jobs require persons with competencies such as problem-solving and critical thinking skills, digital forensics, intrusion detection and incident response, network penetration testing, as well as operating systems and network analysis. The fact that new operators ought to complete extensive training for the satisfaction of ongoing skills' certification, means that the often-witnessed early career burnout and turnover are quite costly for companies and the government. Cyberspace operations such as command and control are regarded as highly demanding cognitive domains that contribute to the highest workloads. Such cognitive workload that entails executing various offensive and defensive cyberspace operations in support of military objectives may hinder sound judgment and cause an escalation of cybersecurity threats.

Cognitively demanding tasks are prevalent in the cybersecurity operations and demand the use of the human operator's visual perception, memory, and attention. They often create a cognitive workload that leads to increased fatigue and errors, which may reduce or impair operator suspicion of malicious activity and lead to an unprecedented, damaging, adverse event in the cyberspace. For example, the friendly fire incidents among US troops in the Gulf War of 1991 were established as being propagated by anxiety and stress, coupled with poor situational awareness (Paul & Dykstra, 2017). The cybersecurity tasks require vigilance that is also associated with cognitive workload, and due to the length of these tasks in terms of time needed to keep watch, the human operators increasingly suffer from fatigue and stress that leads to errors in perception of threat risk, as well as reduced performance. Judgment is often compromised under stress and a heavy cognitive workload, which means that the human operators may fail to identify or establish suspicious cyber activities that amount to cybersecurity threats and propagate attacks. Mental exhaustion, in any field of work, regardless of the rewards has been associated with impaired task performance and the same conceptualization can be applied to the cyberspace. In fact, occupational stress for the human operators as they seek to detect and deter cyber-attacks, leads to cognitive overloads, especially where unmanned crafts and systems are in the security space and pose increased threats or real-time attacks that can escape the fatigued operator's suspicion.

The sparse literature on cognitive workload in cyber defense shows that the length of vigilance demanded for the completion of tasks is mostly responsible for affecting perceptions and performance on the job. A lot of concern has been expressed regarding operators who play a tactical role and are closest to the defense network since they take on the highest risk from complex tasks to adversary skill and knowledge that may overwhelm them mentally (Dykstra & Paul, 2015). With the amount of cognitive workload that is demanded as operators interact with machines, it is unfortunate that this human factor then forms a weak link in cybersecurity, making the systems more vulnerable to attack. The assertion here is that in spite of the training and recruitment of cyberspace operators, the complex environment in which they work and the overwhelming cognitive workload might interfere with their capacity to recognize the threats and cause a human error that will facilitate a cybersecurity incident (Dawson & Thomson, 2018). There are many facets of daily life over which the cyber domain is responsible and the complexity of the cyberinfrastructure, as well several vulnerable devices, continues to grow exponentially. These attributes of the cyberspace have meant heavier mental or cognitive workloads on the cybersecurity workforce that supports this infrastructure while defending the networks, calling for more studies on the impacts of such workloads and the possible solutions.

In the definition of work roles and training in cybersecurity, the Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) developed the Cybersecurity Workforce Framework, which although providing a base set of work roles for the cybersecurity workforce, does not foster teamwork or collaborations (Dawson & Thomson, 2018). The void space in the sharing of aptitudes, skills, and knowledge in the cybersecurity workforce has also contributed to enormous cognitive workloads on individuals, reducing their alertness to suspicious activity and increasing the likelihood of cyber-attacks. According to Dykstra and Paul (2015), operator stress has increasingly become commonplace, propagated by the persistent and disabling effects of cyber operations and heavy cognitive workloads. Operator stress and the subsequent employee burnout have become important risk factors in the performance of cybersecurity workers and the safety of the systems they are manning. Cybersecurity is increasingly being regarded as a high-risk, high-reward profession that can negatively impact its technical workforce or operators manning the systems, through excessive workload pressures that may deter their capacity to detect malicious activity in the cyberspace and cause cyber-attacks (King et al., 2018). Therefore, as humans design and execute cybersecurity programs, they should factor in the spread of the cognitive workload to ensure that it is equitably shared among workers manning the tactical cyber operations.

The ease of measurement of operator error and mission success has shed light on the importance of considering operator fatigue, frustration, and cognitive workload since they can contribute to technical errors or personnel burnout and eventually increase cybersecurity risk events (Paul & Dykstra, 2017). Most of the literature on this subject shows that cognitive workload that also occasions operator stress is the cause for constant staff turnover and this may cause a shortage in cybersecurity workers and heighten inexperience that distorts operator suspicion. If the workers cannot stay long enough on the job due to stress and fatigue, then none will ever be experienced enough to automatically suspect when things are wrong in the cyberspaces they are manning. This problem points to the need for urgency when addressing cognitive workloads in the cybersecurity workspace to ensure that performance of the job is maintained at high-efficiency levels and abnormal situations are arrested as fast as possible to restore normalcy in the organization's or nation's cyberspace. According to Paul and Dykstra (2017), a consistent, measurable factor about an operation is its length, which matters and ought to be considered because it affects operators regarding long-term fatigue, frustration, stress, as well as cognitive wear and tear that ultimately leads to burnout and turnover. Human factors are critical to the success of missions, and operator efficacy should be increased through a wider distribution of the cognitive workload or mental processes entailed in the cybersecurity operations.

2.7 Propositions from Suspicion and Trust Research

This study makes pertinent reference to literature reviewed and from which pointed to the different definitions and explanations of trust and suspicion. Trust and suspicion research surrounding security systems operators cuts across numerous disciplines including military studies, aviation safety, air traffic control, and cyber research in general. From these key studies that contain the main theories surrounding trust and suspicion, the following propositions were established:

- Operators of unmanned systems should use their suspicion to detect any malicious activity that can lead to cyber-attacks
    - (Gay, Horowitz, Elshaw, Bobko & Kim, 2017)
- Suspicion is confirmed through expert recognition of systems whose security integrity has been compromised
    - (Wang, Yan & Zheng, 2018; Kwon, Liu & Hwang, 2014)

- Operator suspicion aids in the development of interventions to secure such cyber-physical systems as unmanned vehicles
    - (Gay, Horowitz, Elshaw, Bobko & Kim, 2019)
- Trust can be an issue, such as in the military, since operator trust reduces suspicion level and presents room for surprise cyber-attacks
    - (Gay, Horowitz, Elshaw, Bobko & Kim, 2019)
- As suspicion increases the cognitive load of operators, they may falter in their perceptions and efficiency of performance on the job
    - (Dykstra & Paul, 2015; Paul & Dykstra, 2017)

These propositions were pertinent in the definition of the problem and formulation of research questions, and more so, the hypotheses as trust and suspicion are explored in the literature review that establishes the theoretical foundations of the same in operations surrounding cybersecurity.

III. Methodology and Design of Experiment

3.1 Chapter Overview

The chapter offers a description of the methodology and experimental design applied in addressing the hypotheses and research questions from chapter 1. The chapter offers insights regarding the models applied in the analysis of different variables regarding the application of the theory of suspicion related to operator detection and the response to the possible cyberattacks on unmanned systems. The chapter also provides an interview with one of the students in AFIT from the system engineering department, and his job was a Ground Control Station Operator (GCSO) in his team. Hence, the chapter describes the tests applicable in ascertaining the relationship between the various variables and the link to the theory of suspicion as identified.

3.2 Methodology

The focus of the research is linked to the evaluation of the relationship between the detection and ensuing response to cyberattacks on unmanned systems and the role of operator suspicion. As identified earlier, suspicion can be broken down into three distinct components that include perception of malicious intent, increased cognitive activity, and uncertainty. The three components occur simultaneously to facilitate suspicion among operators who are then responsible for initiating the needed mitigation mechanisms against the attacks on unmanned systems. The use of the experimental design for the study provides the needed framework for the collection of the data needed in testing the hypotheses and answering the research question.

3.3 Design of Experiment (DoE)

Hypothesis testing incorporated data attained from a survey on active duty Air Force Squadrons. The US and other distinct locations across the world took part in the survey with

3,174 persons from 52 different units taking part in the process. Each of the units contained two hierarchical levels in their arrangements. A large number of the squadrons entailed a total of 10-50 persons. 10% of the total number represented those in leadership positions with a commander taking charge of the entire unit.

The utilization of the Air Force squadrons in testing the proposed hypothesis revolves around identified basic reasons. One of the aspects is the hierarchical organization of the military ranks acting as a pointer of a person's level. Besides the organization, the focus on a specific mission by the squadrons as supported by the unique structure is another major element. Also, military procedures entail individuals traveling temporarily to undertake particular actions and strategies and as such incorporate interactions between the leaders and followers. Lastly, the military setting is characterized by numerous consistent training sessions leading to advanced continuing in the operations. Therefore, the analysis level is an appropriate approach compared to theory testing. The variations linked to the constructs of interest is likely to emerge from the particular individual unit member differences as opposed to the external factors. The target population used in the research study was approved by the Air Force Survey Office, where individual squadrons were selected to act as the sample group. The study used 42 to 130 individuals to collect the necessary data and information. 1,156 military personnel completed the survey where the researcher attained a 49.2% response rate. The participants were allocated distinct segments with each of the unit controlled by a commander. Each squadron availed an average of 30 persons. Notably, 39% of the individuals taking part had been physically separated from the supervisor daily. It meant that they no longer had the mandate to perform their tasks.

The study used the Likert system to accord ranks to all the items. A seven-point Likert-scale itemized the constructs. Scale 1 showed that an individual strongly disagreed to an approach, while the seven ranking level portrayed that the participant strongly agreed with an aspect. All the elements incorporated in the research depicted reliability (e.g., Cronbach's αo > .881).

The human-in-the-loop experiments were conducted in three stages as elaborated below. Stage one entailed obtaining consent from the military, which included collecting personal information from the thirty-two military operators. Additionally, the stage also included collecting information though demographic data and personality-related questionnaires. The second stage aimed at familiarising the participants with the experimental activities through demonstrations and instructions. The stage was necessary in ensuring that an acceptable level of fluency was maintained during the operation. The third stage was characterized by randomly presenting the participants to a series of eight mission scenarios. Each pair was equipped with a pair of mission videos and mission briefings. After completing the mission briefings, the participants responded to the videos events that transpired during each mission scenario, where the response times and response selection were recorded simultaneously.

Upon the completion of each mission segment, through NASA TLX and SSI questionnaires, the participants' malicious intent, uncertainty, and cognitive workload during the mission was obtained. The mission briefings and mission videos were significant to the operator, as they described the mission type, descriptive profiles, and mission context for the unmanned ground vehicle system (UGVS) operations. There were two types of mission, training mission, and operational mission that involved transport and re-supply. The mission contest was set in the Middle Eastern locations or the U.S based on the corresponding estimates of past cyber-attacks. The mission profile was critical in configuring the UGV behaviours. After profile deployment, the UGVS ran autonomously, which generated mission views for playback to be used in the simulation experiments. Visual and verbal mission scenarios were designed to indirectly manipulate the operator's state-suspicions through generating two independent variables. The independent variables were malicious intent and uncertainty that were formed into a two-level full-factorial design.

3.4 Sample and Data Collection

The orientation briefing was completed before transitioning and tasking the members to record and monitor the speed of the Unmanned Ground Vehicle (UGV) after every thirty seconds while being alert to the ongoing activities through video and other instrument readouts to identify anomalous events based on the mission of the UGV. The detection of any anomalous events contributed to the participants being prompted to select and apply the best response from a distinct decision tree that offered a range of various operator responses in times of crises. The tasks were further closely related and aligned to the typical UVS operator tasks while completing questionnaires. The questionnaires completed included the NASA TLX questionnaire that is used in the quantification of the operator's self-assessment based on the cognitive workload on various dimensions that are rated on a scale running from 0 to 100. Secondly, a 13-item SSI questionnaire was provided for the research to evaluate the perception of uncertainty, malicious intent, overall suspicion, and cognitive activation. A 7-point Likert scale was used for the Air Force officers where the experiments took between 2 and 2.5 hours as numerous concurrent operations were ongoing in the office environment. The findings are represented in the **Table 1**:

Table 1: Elements and Reliabilities

Element	Number of Questions	Cronbach’s α (Reliability)
Trust	16	0.75
NASA TLX	6	0.839
Creativity	2	0.57
Suspicion SSI	13	0.881
Cognition	18	0.866
Perception of Consequences	256	0.604
Perception of Uncertainty	256	0.251

The Interpersonal Trust in a Leader

The element of trust is important in operator suspicion, and based on McAllister’s (1995) eleven items of affect and cognition-based trust scale, it was possible to combine the elements to measure the level of trust. The sample items were based on the expression on the shared relationship between the operator and the supervisor regarding the ease of sharing ideas, hopes, and feelings that represent the affect-based characteristics. On the other hand, the measure was based on the supervisor’s track record where the operator could not see a reason to question or doubt the competence of the supervisor nor the preparedness for the job as part of the cognition-based aspect of trust. The Cronbach’s α = .75 supports the conclusions made regarding the influence of trust among operators.

Justice Climate

The justice climate was investigated based on Colquitt's (2001) informational justice, interpersonal, and the thirteen procedural items that offer a picture of organizational justice. Notably, the referent-shift approach was effective in the creation of the items for testing, including questions regarding the handing down of decisions to reach everyone and the treatment of people involved in the squadron with dignity. The justice environment was interrogated at the unit level as the means of ascertaining the elements that contribute positively to operator suspicion. The measure of the justice climate selected for the study was consistent and reflected Naumann and Bennet's (2000) framework that applied procedural justice items alongside the inclusion of interactional items that related to the reasons behind various decisions linked to individuals. The calculation of the values from the test contributed to a finding of Cronbach's ɑ = 0.839.

Affective Organisational Commitment

The measures of creativity identified from the test alongside suspicion and cognition resulted in Cronbach's ɑ= 0.57, 0.881, and 0.866 respectively. The results were okay based on the number of samples being used and highlight the significance of various elements in raising operator suspicion when dealing with threats to unmanned systems. Other areas of interest include the perception of the consequences resulting from operator suspicion and obtained a Cronbach's ɑ= 0.604. The perceptions of the uncertainty was low with a score of Cronbach's ɑ= 0.251. The scores resulted from the research grading the HMT performance while the time aspect indicates the researcher's grading of the operator response time as the means of mitigating against possible adverse effects on the unmanned systems. The calculations were supported by various established models as exemplified by the trust in a leader component. The controls employed in the analysis underline the possibility of effect on the development of interpersonal trust in a leader the interpersonal trust in a leader differentiation. Notably, it was important to understand the significance of the research and effects of operator suspicion in averting possible attacks on unmanned systems.

3.5 Operator Interview

To provide a brief explanation of my thesis regarding Operator understanding and behavior toward operating, I did an interview with one of the students in AFIT from the system engineering department. The student is an international officer who is taking a class in UAV test and evaluation. His job was a Ground Control Station Operator (GCSO) in his team. Also, he was a control officer operating F-16 Aircraft flying missions in Royal Bahrain Air Force (RBAF), so he got experience in real life for both situations. The first situation is operating F-16 Aircraft by being in Ground Control Station (GCS), where the second situation is being an Operator of UAV during class flight test.

The essential focus of my research and this interview was to understand and evaluate the relationship between Operator suspicion and physical system performance and many potential factors that impact while flying such as emotion, trust, cognitive ability, creativity, and situational awareness as show in figure 2.

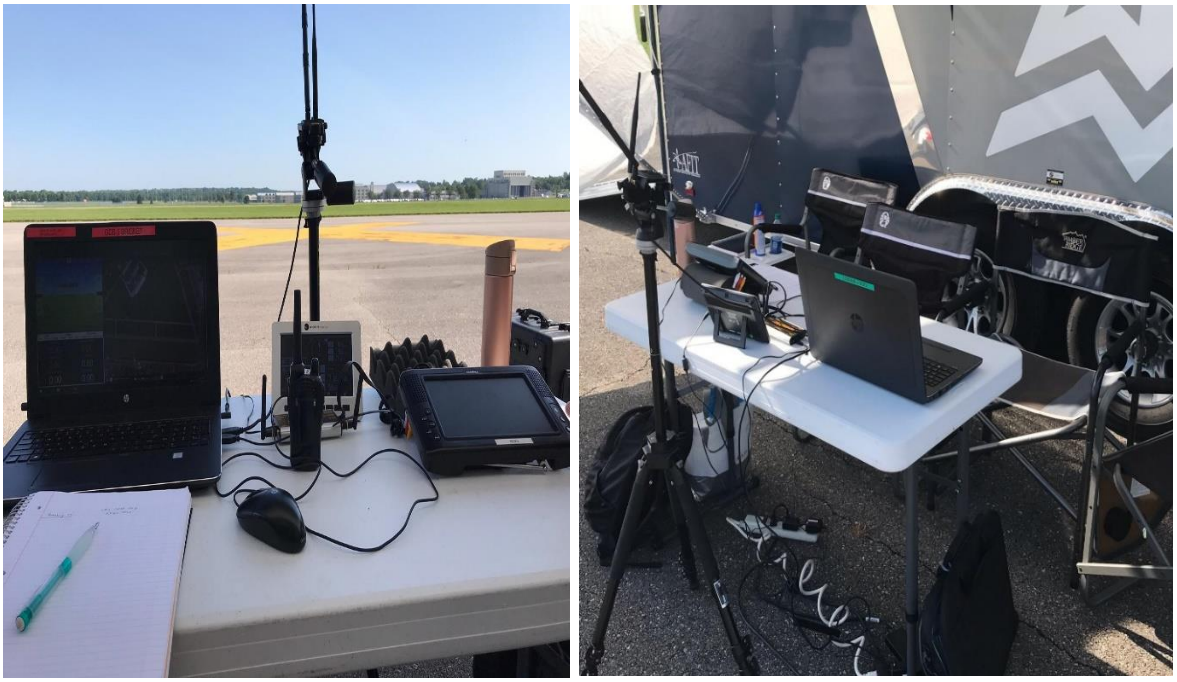


Figure 2: Ground Control Station

3.6 Interview Summary

The interview was beneficial for me in an Operator position so I can understand the operator suspicion and trust. Also, I recognized from this interview that, the operators in the military, for example, receive training on the need for trusting the system as opposed to the necessity of creating suspicions that could be used to deal with possible threats that might affect the system.

3.7 Analysis Approach to Focus and Supplemental Question

The focus research questions (denoted as FRQ) that I focused on were as follows:

- **FRQ1:** What is the significance of operator suspicion and the detection and response to cyber-attacks on unmanned vehicles?

This question was important to set the critical analysis in motion as it gave room for defining operator suspicion and its role in responding to cyber-attacks on unmanned vehicles.

- **FRQ2:** How do trust and suspicion relate to each other? Are they at opposite ends of the same construct, or do they act independently of each other?

  These interlinked questions looked at the aspects of suspicion and trust as opposites of a construct that promote different ends in operator attitudes towards cybersecurity of unmanned systems.

The other questions (denoted as SQ – Supplemental Question) that supplemented the FRQs went further to explore dimensions of suspicion theory with focus on an aspect that is pertinent to operators of the security systems.

- **SQ1:** How do the dimensions of suspicion (uncertainty, malintent, cognitive activation) relate to operator performance? Which dimensions have the largest impact on operator performance?

  These interlinked questions looked at three suspicion dimensions and established cognitive load as bearing greatest impact on operator performance.

- **SQ2:** How do the dimensions of suspicion impact cognitive workload? How is cognitive workload affected by suspicion, trust, and personality?

  Here, cognitive workload was explored deeper as a suspicion dimension that largely impacts operator performance and perceptions.

3.8 Chapter Summary

The methodology and design provided insights regarding the steps taken to establish different parameters related to operator suspicion as exemplified by the investigations and scores on trust and uncertainty, among others. The model used provided a depiction and the platform for the analysis and its linkage to the theory of suspicion as the means of fostering improved monitoring and vigilance. The research design was adopted to ensure the ease of completing the study based on the use of human subjects in the experiment. The interview provided to evaluate the relationship between Operator suspicion and physical system performance, So Identifying cyber-attack is not easy at any jobs during observing operation. Also, the interview illustrated the analysis to the theory of suspicion as the means of encouraging improved observation. So, training Operators for situation awareness with the enhanced alert notification system can be one of the solutions to detect an early clue in any security job.

IV. Discussion and Analysis of Results

4.1 Chapter Overview

The research was designed to investigate the influence of operator suspicion in the detection and subsequent response to cyberattacks that unmanned systems are exposed to in various contexts. The research questions and hypotheses as established in chapter 1 provided the direction of the empirical testing based on the methodology outlined in chapter 3 with the experiments designed to probe the influence of operator suspicion as identified in each of the questions and hypotheses. The chapter offers an analysis and evaluation of the data from the research based on the responses of active duty Air Force officers who represent the operators of the Unmanned Ground Vehicles (UGVs). The chapter highlights the findings based on the data generated from the experiments targeted at answering the hypotheses and research questions.

4.2 Research Questions and Hypotheses

The research questions and hypothesis could be distinguished into two broad categories with one including those associated with the suspicion theory and its influence on operator detection and response to possible cyberattacks on unmanned systems and the second group including those related to the theory itself. The questions related to the theory of suspicion based on the actions of the operator are classified as focus research questions (FRQ) and hypothesis (FRH) as highlighted in chapter 1. The robustness of the experimental design facilitated the collection and analysis of data related to the theory of suspicion based on the supplemental questions and hypothesis denoted as SQ and SH respectively. The following two sections offer a discussion of the experimental findings from the two categories described based on the distinction of the research questions and hypotheses.

4.2.1 Analysis of the Focus Research Questions and Hypotheses

The following focus research questions were applied regarding the suspicion theory in relation to operator detection and the subsequent response to cyberattacks on unmanned systems as denoted using (FRQ).

1. **FRQ1**: What is the significance of operator suspicion and the detection and response to cyberattacks on unmanned vehicles?
2. **FRQ2**: How do trust and suspicion relate to each other? Are they at opposite ends of the same construct, or do they act independently of each other?

The research questions are subsequently linked to their focus hypotheses as shall be highlighted in this section.

1. **Focus Research Question 1 (FQR1):** What is the significance of operator suspicion and the detection and response to cyber-attacks on unmanned vehicles?

The research question was important in setting the critical analysis in motion as it provided the needed rom for the definition and understanding of operator suspicion and the role in the response to cyberattacks on unmanned vehicles. The performance was measured based on the distinct components that included Time and Score as each was recorded and calculated independently in the identification of the operator's response to a particular mission. The Score offered a reflection of the decision-making component of the performance while the Time served as the reflection of the length of time required while arriving at the important decision to intervene.

Summary of the FRQ1 Findings

The results indicate that operator suspicion had a notable impact on the HMT performance as noted based on the focus research hypothesis (FRH), particularly FRH .1.1 and

FRH .1.2 on the detection of cyberattacks on UAVs and the speediness of the response to the suspicious activity. The results further indicate that the operators' responses to tasks and response to sequence selections were linked to low performance based on the increased level of suspicion. Notably, the different cyberattacks and sentinel combinations were tested to assess the impact on the suspicion levels of the operators. The operators were strongly influenced by the likelihood of occurrence of sentinel and cyberattack activities as demonstrated in the findings of the study.

4.2.2 Analysis of the Focus Research Hypothesis for Focus Research Question 1

The hypothesis related to FRQ1 were denoted as FRH1 and included four hypotheses to identify various parameters of the study, including operator suspicion on the detection of cyberattacks on UAVs and the speed in the response to suspicious activities.

FRH .1.1: Operator suspicion is significant in detection of cyber-attacks on UAVs

According to Bobko et al., environmental cues are important in the trigger of the alert level and suspicion and can be classified as sentinel alerts as the operators become sensitive to abnormalities in the system. Bobko et al. indicates that negative discrepancies, distrust, and missing information are important factors that contribute to suspicion. Further, suspicion contributes to the greater search for information and the consideration of multiple ways that attacks can be perpetrated. I hypothesized that operator suspicion was significant in the detection of cyberattacks on UAVs. The findings from the correlation analysis indicate a positive Score that highlights the positive relationship between operator suspicion and the significance in the detection of cyber-attacks on UAVs. The results from the correlation analysis are presented in table 1 in the appendix and indicate a positive score of 0.57. The hypothesis FRH .1.1 was supported by the findings as suspicion was found to correlate at the 0.01 level to the detection of cyber-attacks. The results are further supported by the interview I conducted as the respondent indicated that he felt suspicious despite the existence of firewall protections tin the system as part of human nature. Therefore, it indicates that suspicion is an important component in the detection of potential attacks on UAVs. This relationship was described graphically in Figure 3.

PERFORMANCE AS A FUNCTION OF OPERATOR SUSPICION

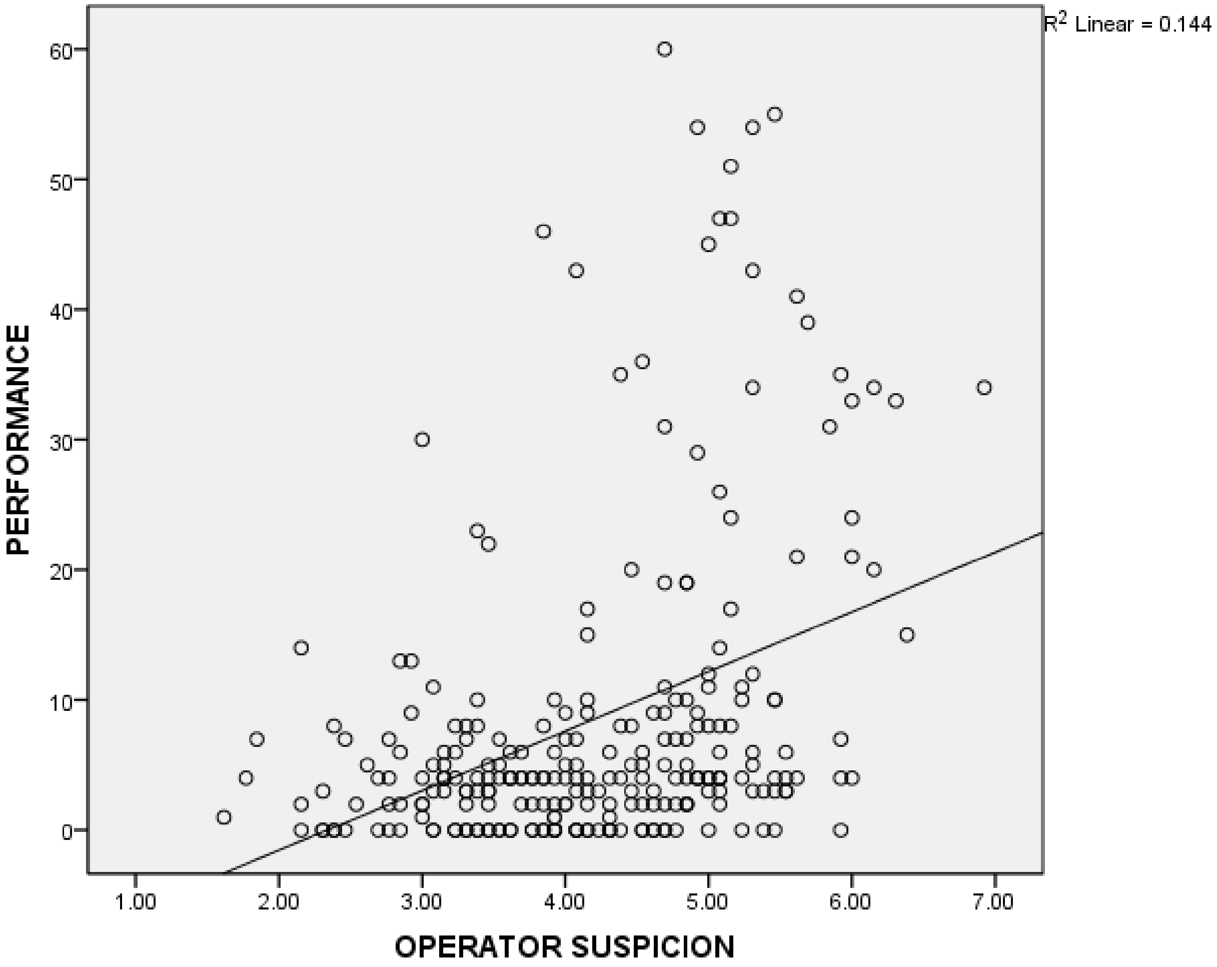
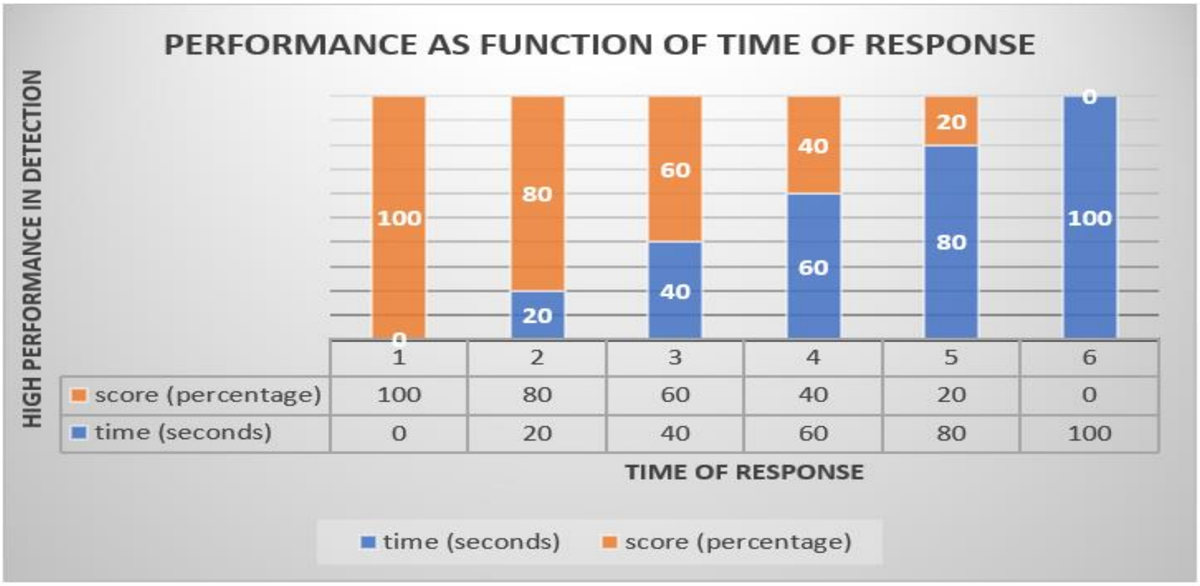


Figure 3: Graph of HMT performance as a Function of Operator Suspicion

FRH .1.2: Detection is positively linked to the speediness of response to the suspicious activity.

Detection is an important aspect related to the response time required to deal with suspicious activities. It is important to note that cyberattacks are malicious, and hence require early detection as the means of ensuring measures are taken in a timely manner to avert possible calamities. Operator suspicion is linked to the greater search for information and the increase in the active procession of information that contribute positively to the operator response time. I hypothesized that detection was positively linked to the speediness of the response to suspicious activities. The results from the correlation table indicate a positive score for the time component indicating a direct relationship between detection and the timely interventions to avert cyberattacks. The direction of the relationship was negative implying that low detection impact delay in respond which can cause a disaster such as losing the UAVs and can link to adverse events as indicated in the results in table 1 in the appendix. This relationship was described graphically in Figure 4.



	1	2	3	4	5	6
🟧 score (percentage)	100	80	60	40	20	0
🟦 time (seconds)	0	20	40	60	80	100

Figure 4: Graph of HMT Performance as a Function of Time of Response

2. **FRQ2:** How do trust and suspicion relate to each other? Are they at opposite ends of the same construct, or do they act independently of each other?

The interlinked questions are important in exploring the various aspects of suspicion, including the identification of whether trust is an opposite construct that facilitates the promotion of different ends in operator attitudes towards cybersecurity of unmanned systems. The various components of suspicion were measured to determine whether they were at opposite ends of the same construct or they functioned independently.

Summary of Findings for FRQ2

The influence of suspicion and trust in determining the response of operators cannot be overstated. The two, suspicion and trust, are interrelated and do not act independently but rather are at the opposite ends of the same construct. Trust and suspicion are influential in the determination of the course of action that operators pursue regarding cyberattacks on unmanned systems. The interview revealed some link between suspicion and trust as the respondent strongly reported that he did not trust the system at all based on the capabilities of hackers while further asserting that he was highly perceptive and suspicious as a human about the capacity of the protections for the system to avert cyberattacks. Similarly, the results from the correlation analysis signified the strength of the relationship between suspicion and trust.

4.2.3 Analysis for the Focus Research Hypothesis (FRH) for FRQ2

FRH.2.1: Trust and suspicion are related.

FRH.2.2: They are inversely related as opposite ends of the same construct.

For the two hypotheses, I sought to explore the relationship between trust and suspicion as exemplified by the first hypothesis where I hypothesized that trust and suspicion were related. The results from the correlation analysis indicated a positive relationship on the McShane scale while the Mayer's scale indicated no relationship between trust and relationship. Trust Mayer's scale yielded a negative figure of -0.076 compared to the positive score of 0.791 for the Trust McShane scale. The correlation scores indicate the summative effect being negative further not supporting the hypothesis as the trust and suspicion were not directly related but rather had a negative relationship.

On the second hypothesis, a correlation that was greater than 0.90 indicating the inverse relationship between trust and suspicion of the same construct. The findings support the hypothesis and underline the trust and suspicion as being inversely related as the opposites of the same construct. This relationship was described graphically in Figure 5.

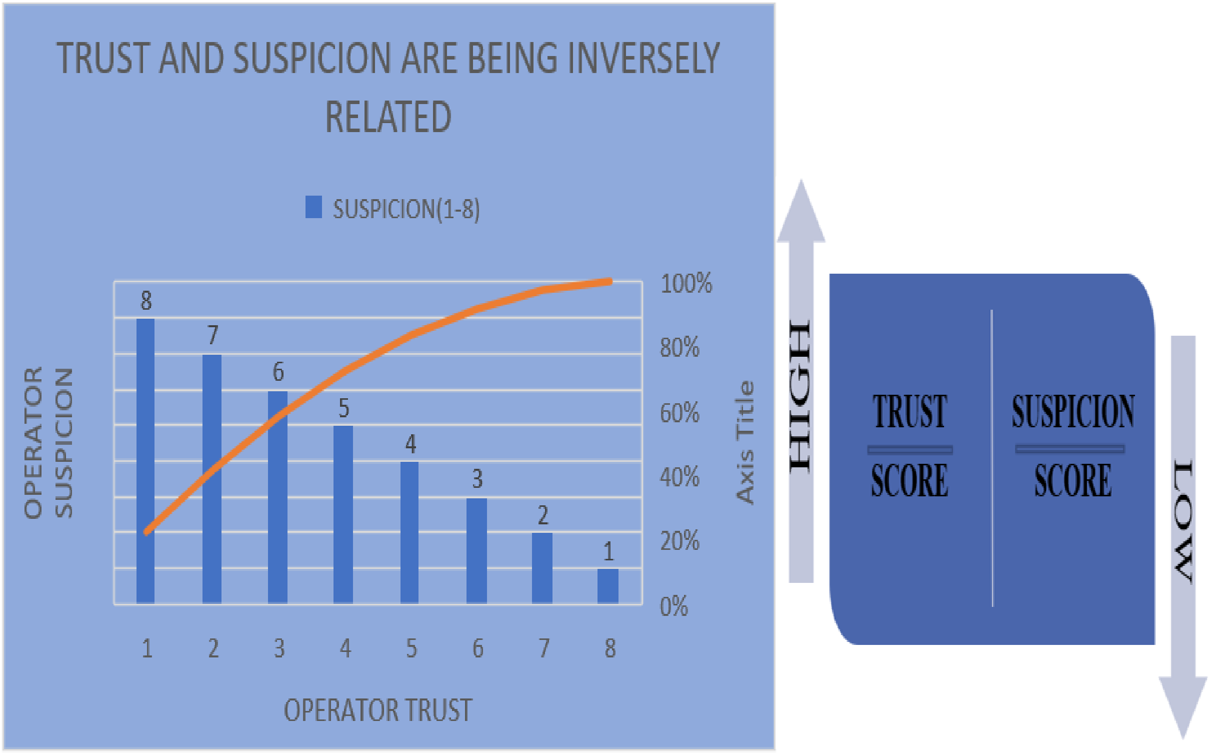


Figure 5: Graph of the Relation of Trust and Suspicion

4.2.4 Supplemental Questions

The other questions (denoted as SQ – Supplemental Question) that supplemented the FRQs went further to explore dimensions of suspicion theory with focus on an aspect that is pertinent to operators of the security systems.

- **SQ1:** How do the dimensions of suspicion (uncertainty, malintent, cognitive activation) relate to operator performance? Which dimensions have the largest impact on operator performance?

These interlinked questions looked at three suspicion dimensions and established cognitive load as bearing greatest impact on operator performance.

- **SQ2:** How do the dimensions of suspicion impact cognitive workload? How is cognitive workload affected by suspicion, trust, and personality?

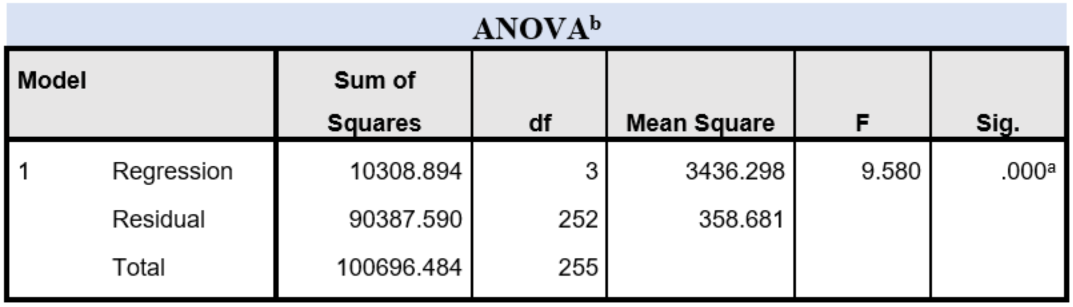
  Here, cognitive workload was explored deeper as a suspicion dimension that largely impacts operator performance and perceptions.

Related to the supplemental questions were the following hypotheses, marked as SH – supplemental hypothesis addressing the aspect of cognitive load in suspicion theory as per Gay, Horowitz, Elshaw, Bobko and Kim (2017), as well as Paul & Dykstra (2017).

- **SH.1.1:** The three dimensions of suspicion negatively affect operator performance.
- **SH.1.2:** Operator performance is largely impacted by cognitive load.
- **SH.2.1:** Cognitive workload is increased by having to differentiate suspicion and trust.
- **SH.2.2:** Personality of the operator towards being highly suspicious or highly trusting positively increase cognitive workload.

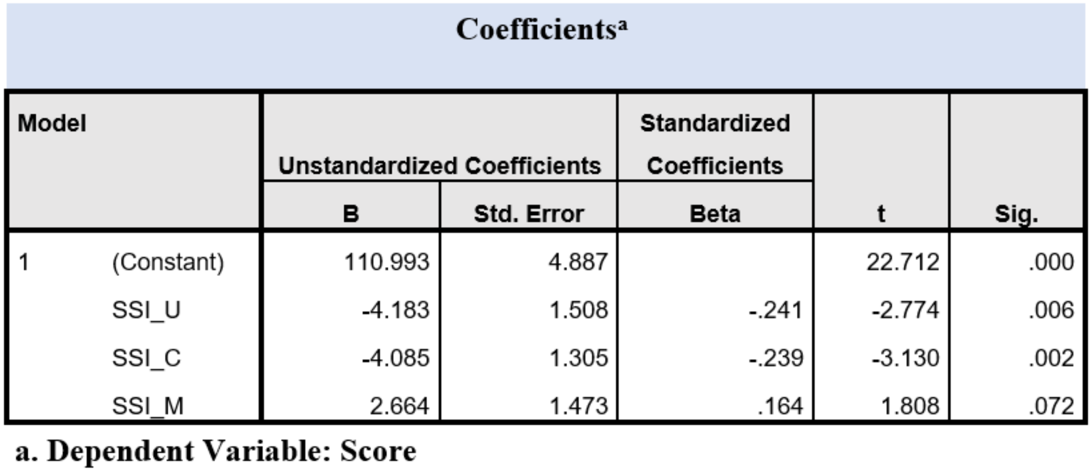
  Based on the regression analysis conducted the first hypothesis was on the three dimensions of suspicion having negative effects on operator performance. The results support the hypothesis and indicate partial support as the three dimensions of suspicion had some level of influence on operator performance based on the prevention of cyberattacks on UAVs. And the data collected was summarized in **Table 2**.

Table 2: Regression Analysis of the three dimensions of Suspicion on Operator Performance



ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10308.894	3	3436.298	9.580	.000[a]
	Residual	90387.590	252	358.681		
	Total	100696.484	255			



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	110.993	4.887		22.712	.000
	SSI_U	-4.183	1.508	-.241	-2.774	.006
	SSI_C	-4.085	1.305	-.239	-3.130	.002
	SSI_M	2.664	1.473	.164	1.808	.072

a. Dependent Variable: Score

Where,

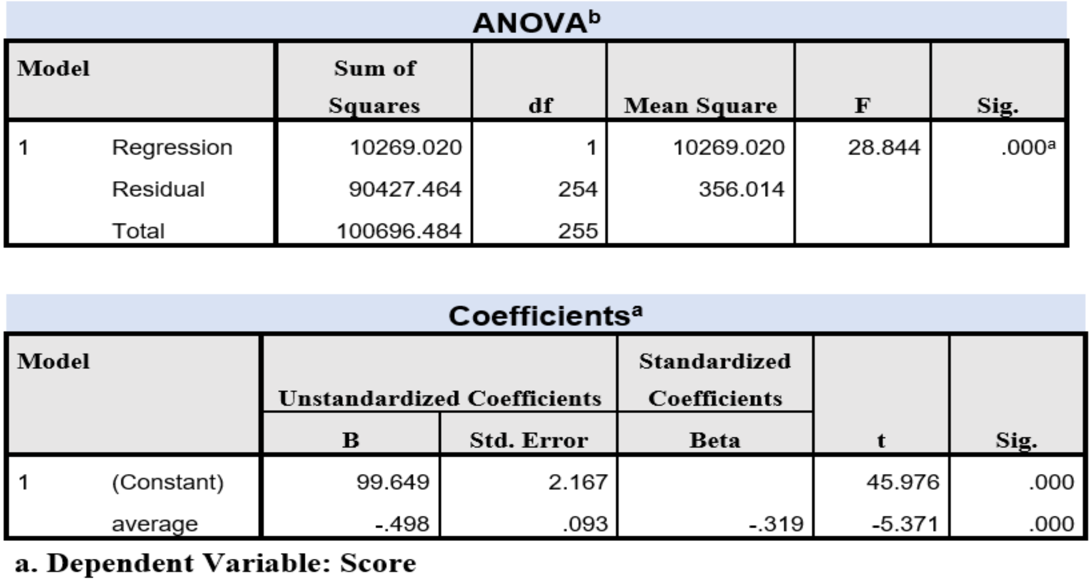
SSI_U: Uncertainty.

SSI_C: Cognitive Activity.

SSI_M: Perceived Malintent.

Similarly, the second hypothesis was supported as the cognitive load has a significant influence on operator performance. And the data collected was summarized in **Table 3.**

Table 3: Regression Analysis of the Cognitive Load on Operator Performance.



ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10269.020	1	10269.020	28.844	.000[a]
	Residual	90427.464	254	356.014		
	Total	100696.484	255			

Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	99.649	2.167		45.976	.000
	average	-.498	.093	-.319	-5.371	.000

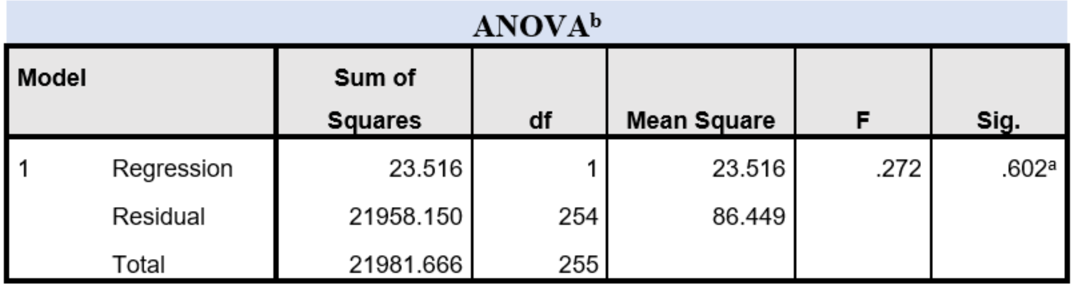
a. Dependent Variable: Score

Where,

TLX_Total_mean: The Cognitive Load

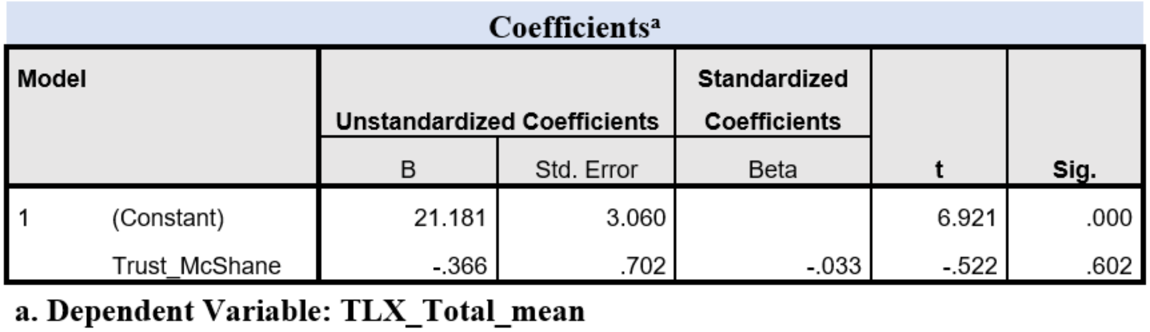
The third hypothesis was not supported as Trust was not significantly related to cognitive load. This makes sense because if you trust an individual, you will not spend any time to cognitively analyze the situation or what you’re being asked to do. And the data collected was summarized in **Table 4.**

Table 4: Regression Analysis of the Trust to the Cognitive Load



ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23.516	1	23.516	.272	.602[a]
	Residual	21958.150	254	86.449		
	Total	21981.666	255			



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	21.181	3.060		6.921	.000
	Trust_McShane	-.366	.702	-.033	-.522	.602

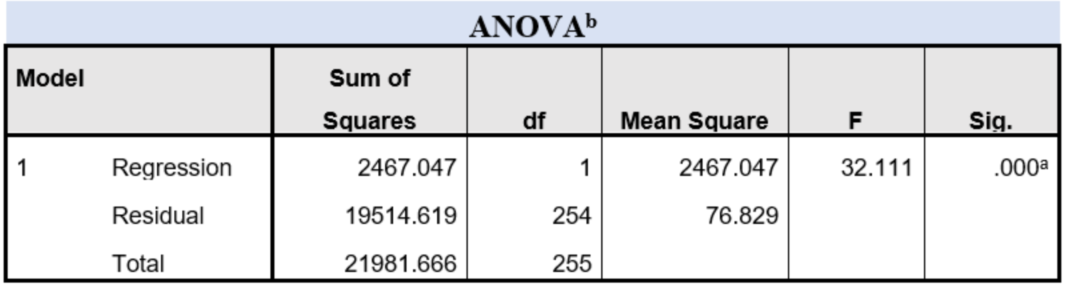
a. Dependent Variable: TLX_Total_mean

Where,

TLX_Total_mean: The Cognitive Load

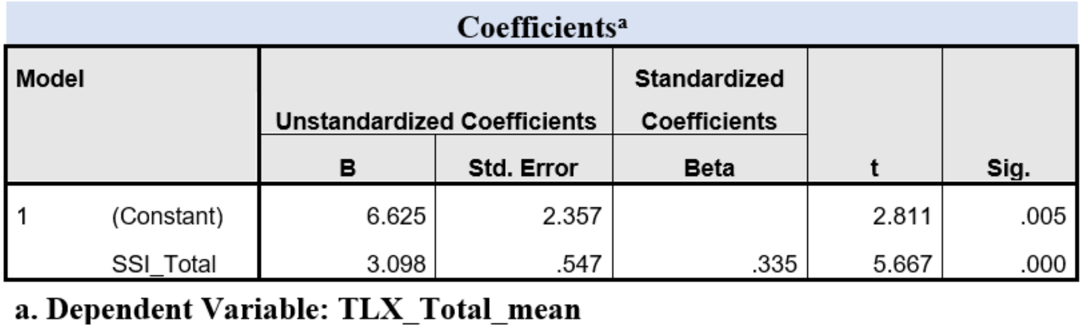
On the other hand, the fourth hypothesis was further partially supported by the results of the regression analysis as suspicion was linked to the increase of the cognitive workload. Hence If you are suspicious of somebody, you will analyze everything they do and say before you decide to take action because you are unsure whether they have your best interest in mind. The more suspicious you are of somebody, the more time you will spend thinking about what actions are appropriate. And the data collected was summarized in **Table 5.**

Table 5: Regression Analysis of the Suspicion to the Cognitive Load



ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2467.047	1	2467.047	32.111	.000[a]
	Residual	19514.619	254	76.829		
	Total	21981.666	255			



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6.625	2.357		2.811	.005
	SSI_Total	3.098	.547	.335	5.667	.000

a. Dependent Variable: TLX_Total_mean

Where,

SSI_Total: The three dimensions of the suspicion theory (uncertainty, perceived malintent, and cognitive activity).

4.3 Research Limitations

As with other experiments, the study had its limitations, particularly the lack of a baseline to measure operator performance based on the scope of the research and limited resources. The results were largely inferential as there lacked the needed baseline to compare the results. The other limitation could be linked to the low sample size to provide results that could be generalized. The sample of N=256 and also the interview with just one person limited the possibility of the generalization of the findings. It was very hard to find a UAV operator to get an interview with because it is confidential job skills in the RSAF and USAF.

4.4 Chapter Summary

The chapter presents the findings from the experiment component of the study that identified the connections between operator suspicion and the detection of possible threats of cyberattacks on unmanned systems. Some of the broad issues considered include the significance of trust and suspicion as the leading components that play an important role in the activities of operators who tend to the unmanned systems. The results support the literature regarding operator suspicion being important in the detection of possible threats and the part played in the timely intervention of some of the challenges faced on unmanned systems.

V. Conclusion and Recommendation

5.1 Chapter Overview

The chapter provides a summary of the dissertation by highlighting its purpose and scope in relation to the literature and findings. Further, the chapter discusses the research contributions, particularly related to the Royal Saudi Air Force (RSAF) based on the experiment and the interview. Finally, the conclusion focuses on the future work as the means of extending the impact and relevance of the research.

5.2 Review of Purpose and Scope/Summary

As outlined in the research, the focus was on the establishment of the relationship between operator suspicion and the detection and response to cyber-attacks on unmanned systems. The different chapters from chapter 1 to 4 covered the introduction, literature, methodology, and discussion and analysis of results respectively. The research provided the background of the study based on previous studies as exemplified in the introduction that looked at the theories related to suspicion, theoretical model, and the research questions and hypotheses. The framework and background provided in the first chapter were important in the literature section that reviewed existing literature on operator suspicion and the link to the detection of possible attacks on unmanned systems. The third chapter described the methodology used in the research as the foundation for the interview and experiment based on the research questions and subsequent hypotheses.

The importance and increased use of unmanned systems for security purposes, particularly in the military, contributed to the need for the research that focused on analyzing the cyber-attacks that are targeted at the cyber-physical systems (CPS) of unmanned vehicles. Significant research on the subject further contributed to the interest in the topic as the emergent threats on unmanned systems have significant and catastrophic risks on security systems. Research has corroborated the importance of the topic as exemplified by the increment in the investments from the Royal Saudi Air Force (RSAF) and United States Air Force (USAF) in unmanned systems used for armed attacks, border surveillance, reconnaissance, and transportation. Therefore, the findings from the previous research work served as the motivation for the study to analyze the effects of operator suspicion on the detection and response to cyber-attacks. The need for the implementation of measures on the identification of the methods used by hackers in accessing unmanned systems has been highlighted as part of the motivation for the study.

The research framework used places significant emphasis on the timely interventions based on suspicious activities that could threaten the functioning of unmanned systems. Therefore, based on the backing of research, it was important to explore the significance of suspicion in the military setting as operators in the military receive training that enhances the need for trusting systems as opposed to the creation of suspicion. The trust levels of military personnel in systems contributes significantly to the increase in the risks that unmanned systems are exposed to and reinforced the need for the research. The use of the suspicion theory was pivotal as the framework that can be applied in the exploration of the means through which operators detect and initiate response mechanisms to deal with cyber-attacks on unmanned aerial and ground vehicles. The issues highlighted, particularly regarding suspicion and trust in the military, contributed to the need for the research and the literature review to understand the application of suspicion theory in the examination of improvements that can be achieved in operator detection and the response to possible cyber-attacks on unmanned systems. The high mission demand and the subsequent operational tempo created limitations on the use of actual

Unmanned Aerial Vehicle (UAV) Operators, but the use of literature and the emulation of the context were significant in the exploration of the possible solutions and the experiment. Research indicates that the majority of the cyber-attacks are not instantaneous and are characterized by resource-intensive and time consuming activities. Therefore, the understanding of the element of cyber-attacks contributed significantly to the research direction and experiment and the exploration of the security that could increase the preparedness of operators. The Suspicion theory as identified by Bobko was an important component of the theoretical model applied in the research targeted at the understanding of how operators detect and respond to cyber-attacks on unmanned systems.

5.3 Research Contributions

The effects of cyber-attacks on cyber-physical systems cannot be overstated with the emergent threats having significant impacts, particularly on security installations and missions. The topic has witnessed increased research attention in addressing the physical security aspects related to unmanned systems. Therefore, the research addressed the human component of cyber-attack detection and response among operators, particularly in the military setting. The research combined aspects of trust and suspicion as the means of establishing the approaches that can be applied in the military setting to minimize the effects of adverse events related to cyberattacks on Unmanned Aerial Vehicles (UAVs). The emphasis on trust in the impenetrability of systems has been identified to create challenges when dealing with unmanned systems as operators have low levels of suspicion and take long to respond to threats. The influence of suspicion in the timely response to threats cannot be overstated as operators initiate measures to deal with possible security breaches and inspection of threats.

The contributions of the research are significant in the training of situation awareness among operators. Notably, the research' findings signal the importance of suspicion, particularly in the military setting as the means of reinforcing the timely response to possible cyber-attack threats. According to the interview, the experience of abnormal activities that includes the loss of communication and Global Positioning System (GPS) failure locations are some of the challenges that confront operators. From the operator's perspective in the interview, it was evident that the loss of communication with the Unmanned Aerial Vehicle (UAV) is a serious issue and could only be justified using assumptions. Notably, the operator indicated some concern about the failures being linked to possible cyber-attacks, and that enhances the significance of the research in highlighting the need for suspicion that can increase the chances of exploration of vulnerabilities. In the absence of suspicion, operators would fail to detect and implement measures to avert security threats associated with cyberattacks. Hence, suspicion creates the room for exploring different alternatives while investigating abnormal events as opposed to cases where operators trust the systems.

The interview further indicated the absence of the required capabilities for the detection of cyberattacks. The research offers important contributions in the identification of the necessity of training of situation awareness for the operators to deal with the challenges identified in the interview regarding the absence of training to enhance awareness. Notably, the majority of the military training schedules emphasize on trusting the systems as opposed to suspicion that could be important in ensuring operators can detect and respond to cyber-attacks in a timely manner. Additionally, the experiment highlighted the significance of suspicion based on the component of time and the response to possible cyber-attacks.

The second contribution of the research can be linked to the building of a security system of notification and alerts that can be part of the cyber department of the Air Force. As identified, the Air Force is limited in its responses to possible attacks on unmanned systems that conduct important security operations. The capacity to minimize cyber-attacks can be linked to training in the Air Force and significance of trust in ensuring military operators are suspicious of the systems and can device measures to respond to possible security threats. My research targeted the reduction of the threats posed against cyber-physical systems, particularly the unmanned aerial and ground vehicle systems used by the Air Force.

The findings from the research experiment, particularly the first research question indicated a positive relationship between operator suspicion and the detection and response to cyberattacks on unmanned vehicles. Additionally, the findings indicated an inverse relationship between trust and suspicions as being on the opposite ends of the same construct. The trust placed on systems contributes significantly to the lower rate of detection, and hence, the research contributes based on the recommendations for training among Air Force operators on the importance of suspicion in enhancing the detection and response to cyberattacks. The cyber department of the Air Force, should therefore, implement security measures to ensure the systems are designed to offer notifications and alerts based on possible cyber-attacks. The results based on the time indicate the necessity of initiating interventions that are time-conscious and contribute to the aversion of calamities. Trust and suspicion are important components that influence the reflection of the length of time required to initiate an intervention.

The research can be implemented by the Royal Saudi Air Force (RSAF) in its adoption and use of unmanned systems that serve different purposes. Hence, the Air Force shall benefit from the application of the research findings in the implementation of proactive training measures for the situation awareness among its operators to be aware of possible cyber-attacks and the necessary responses. My research was uniquely designed where no one did that before in the Royal Saudi Air Force (RSAF) because it offers the needed information to the Royal Saudi Air Force (RSAF) and sets the base for the organization to consider the impacts of the human factor in the sensitive area of operations. The research offers information that can be used in exploring the interventions that can be used to deal with the human factor in the monitoring and detection of strange activities that could reduce the efficacy of Unmanned Aerial Vehicles (UAVs) while completing a mission. The application of the findings by the Royal Saudi Air Force (RSAF) could reduce cases of cyber-attacks that could destroy costly machines, and also subvert the missions that the unmanned systems are deployed to complete.

5.5 Recommendations for Future Research

The study identified the need for additional research to support the findings regarding the need for operator training and awareness regarding the importance of the concepts of suspicion and trust in the detection and response to cyber-attacks on unmanned systems. Future research could focus on the effects of operator suspicion to the performance of the detection and response times without operator knowledge and the challenges faced by possible cyber-attack alert systems. Hence, future research could concentrate on the identification of the cyber-attack alert systems that could complement the human factors involved in the detection and response to cyber-attacks. The cyber-attack detection services are not currently available in the different Saudi Air Force unmanned system and could form the basis for future research that would work on the identification of the possible system responses. Future research should study the effects of suspicion and the consequences of operator performance on the enhanced performance measure where time is a factor. Additionally, another area of research could be the establishment of the type of attack that corresponds to operator suspicion as the means of identifying defined training procedures.

5.6 Chapter Summary

The dissertation relied on literature, an interview, and experiment to investigate the emergent threat of cyber-attacks on unmanned systems, particularly in the military (Air Force). The nature associated with cyber-attacks indicates malicious intent and activities as highlighted by Bobko et al. based on the theory of suspicion. The Suspicion Theory offered the needed theoretical framework supporting the research in the investigation of the link between suspicion and the detection and response to cyber-attacks by operators in the military. One of the challenges addressed concerns the issue of trust that defines the interaction of Air Force operators with unmanned systems. The operators are trained to trust the systems, and therefore, fail to raise suspicion in the detection and response to cyber-attacks against unmanned vehicle systems. The research highlighted the significance of suspicion in enhancing the detection of cyber-attacks among operators in the military setting as the counter-measure to the concept of trust that defines the interactions of military personnel with systems. Operator suspicion forms the basis for recommendations regarding the need for training that enhances the awareness of operators to issues related to cyber-attacks. The propositions established in the research offer the needed information in the exploration of the link between trust and suspicion while dealing with the threats that unmanned systems face.

Appendix A.

Reliability

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.752	8

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.866	18

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.570	2

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.881	13

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.839	6

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.604	2

Scale: ALL VARIABLES

Case Processing Summary

		N	%
Cases	Valid	256	100.0
	Excluded[a]	0	.0
	Total	256	100.0

a. Listwise deletion based on all variables in the procedure.

Reliability Statistics

Cronbach's Alpha	N of Items
.251	2

Appendix B.

Interview questions

Q.1 Did you operate in Unmanned Vehicle and for how long?

Yes, I have been operating UAV during on my class in AFIT at Area B runway for two days of flight test and two missions of 30 minutes of flying for each mission.

Q.2 Did you experience any abnormal activities and behaviors during your job as an Operator?

Yes, I have been experienced some abnormal activities such as losing communication and GPS failure locations.

Q.3 What cause those abnormal activities form your understanding?

I think that we lost communication because the codes that we wrote in the autopilot is not letting the UAV communicating with us. The second problem was the GPS is not working well during the mission. Those assumptions were discovered after the mission in the troubleshooting phase.

Q.4 Can the cyber-attack be a suspicion threat in those cases?

Yes, when those faults occur, I was not sure why the UAV is giving me those faults. A cyber-attack can be a reason behind those abnormal errors.

Q.5 What the capabilities of detecting cyber-attacks? If not, why?

The truth is no capabilities of detecting cyber-attack immediately because we are not training of this kind of situation. Also, the ground control station (GCS) is not capable of detecting those kinds of attacks.

Q.6 Do you trust your system which is the Ground Control Station software of communication and telemetry transfer between the UAV and GCS?

No, I don’t trust the system at all, because the capabilities of the hackers are unlimited from the news feedback all over the world about them.

Q.7 Is there any notification or alarm regarding abnormal activities?

Yes, there are notification and alarm in the mission planer program inside the GCS but without explaining what causes them to fail.

Q.8 Do you feel suspicion even when there is firewall protection exist in the system?

Yes, I always feel suspicion because it is my human nature.

Q.9 when you were observing the operation, is cognitive that you provide in your task is for Maintenance failure or other things such as cyber-attack?

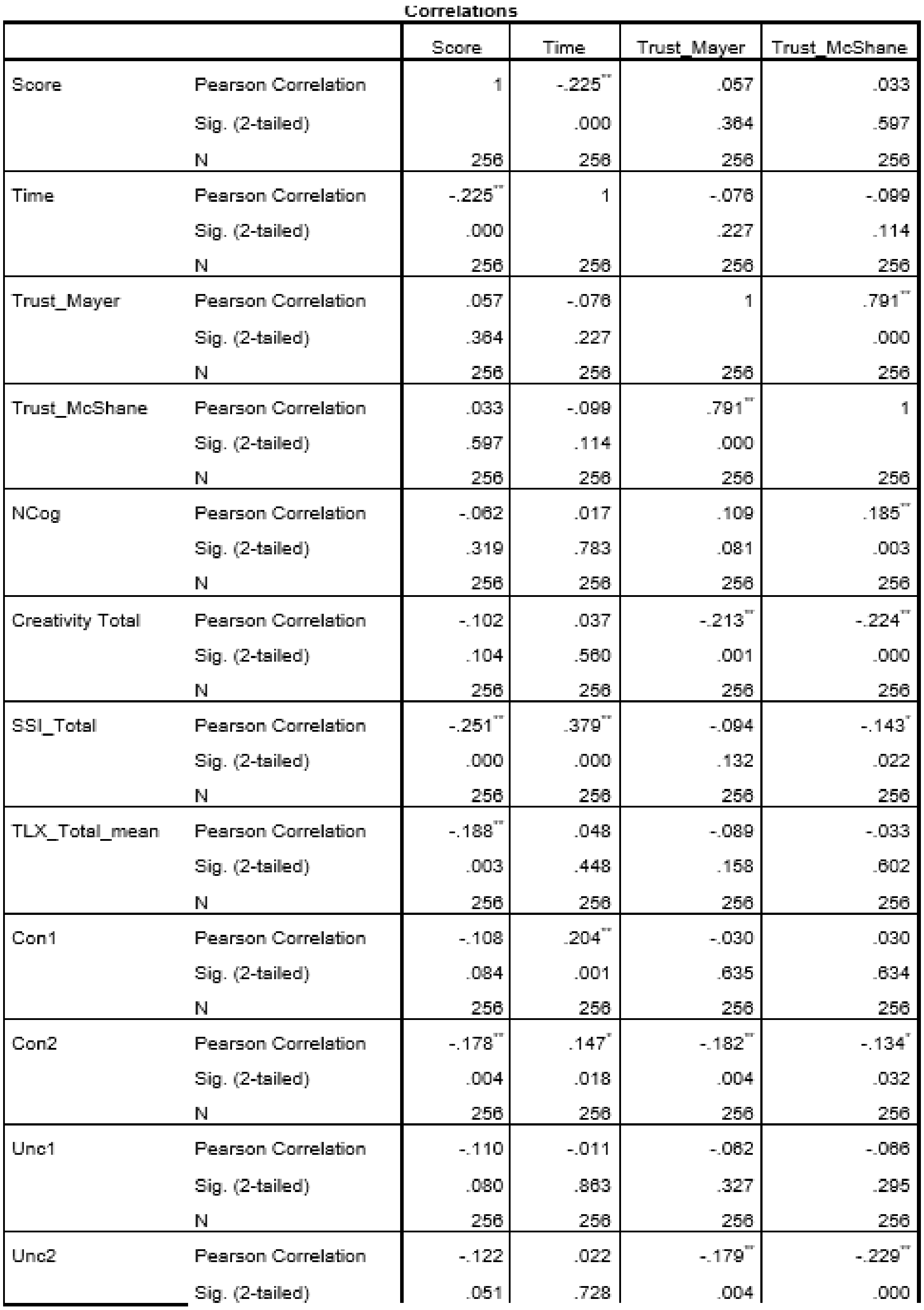
I was only focusing on cognitive toward maintenance failure reasons.

Q.10 Is workload can be a significant cause of low suspicion of cyber-attack and high trust of the system?

Yes, I think that workload can be a major factor of causing low suspicion of cyber-attack and high trust of the system.

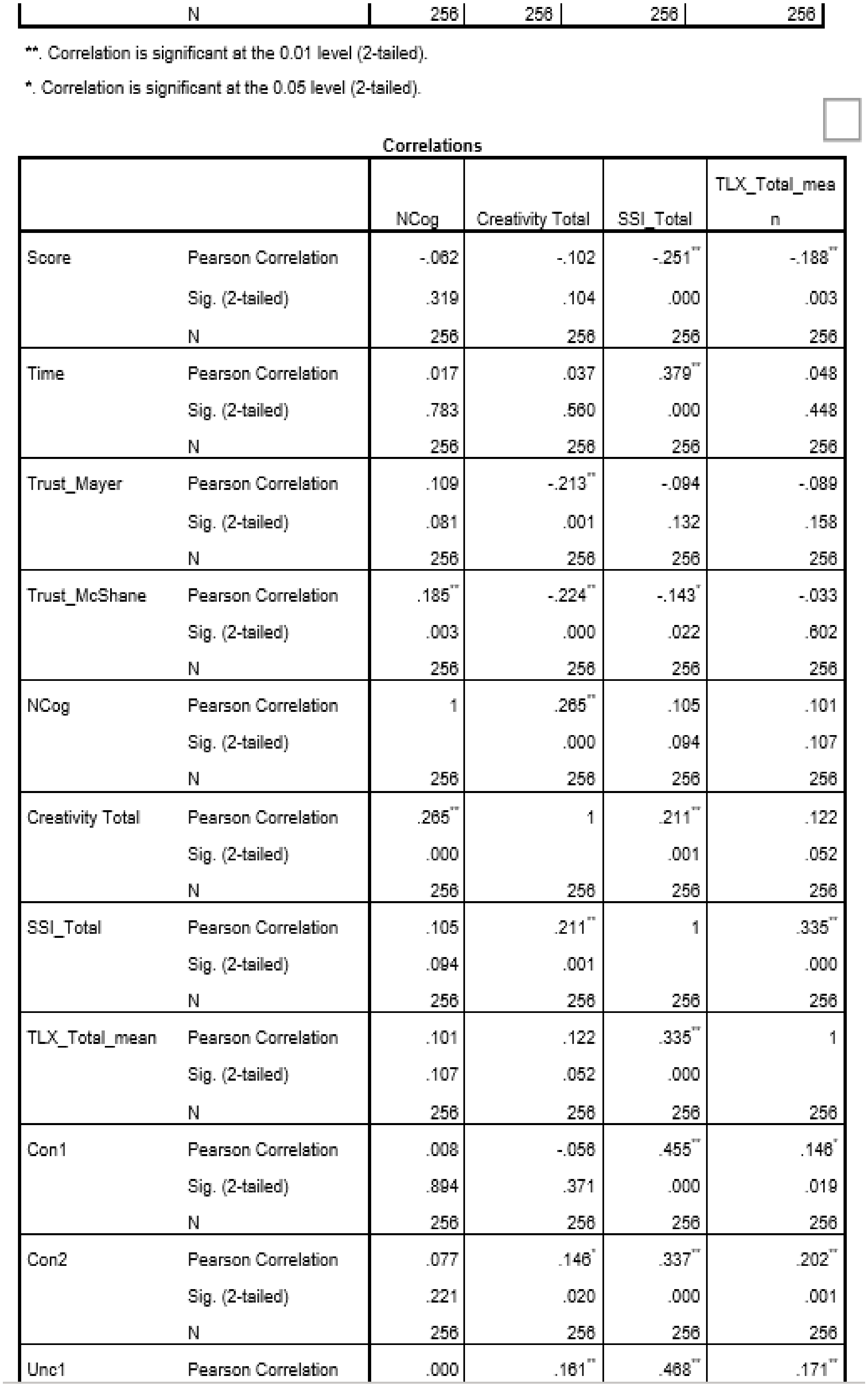
Appendix C.

Correlation



Correlations

		Score	Time	Trust_Mayer	Trust_McShane
Score	Pearson Correlation	1	-.225**	.057	.033
	Sig. (2-tailed)		.000	.364	.597
	N	256	256	256	256
Time	Pearson Correlation	-.225**	1	-.076	-.099
	Sig. (2-tailed)	.000		.227	.114
	N	256	256	256	256
Trust_Mayer	Pearson Correlation	.057	-.076	1	.791**
	Sig. (2-tailed)	.364	.227		.000
	N	256	256	256	256
Trust_McShane	Pearson Correlation	.033	-.099	.791**	1
	Sig. (2-tailed)	.597	.114	.000	
	N	256	256	256	256
NCog	Pearson Correlation	-.062	.017	.109	.185**
	Sig. (2-tailed)	.319	.783	.081	.003
	N	256	256	256	256
Creativity Total	Pearson Correlation	-.102	.037	-.213**	-.224**
	Sig. (2-tailed)	.104	.560	.001	.000
	N	256	256	256	256
SSI_Total	Pearson Correlation	-.251**	.379**	-.094	-.143*
	Sig. (2-tailed)	.000	.000	.132	.022
	N	256	256	256	256
TLX_Total_mean	Pearson Correlation	-.188**	.048	-.089	-.033
	Sig. (2-tailed)	.003	.448	.158	.602
	N	256	256	256	256
Con1	Pearson Correlation	-.108	.204**	-.030	.030
	Sig. (2-tailed)	.084	.001	.635	.634
	N	256	256	256	256
Con2	Pearson Correlation	-.178**	.147*	-.182**	-.134*
	Sig. (2-tailed)	.004	.018	.004	.032
	N	256	256	256	256
Unc1	Pearson Correlation	-.110	-.011	-.062	-.066
	Sig. (2-tailed)	.080	.863	.327	.295
	N	256	256	256	256
Unc2	Pearson Correlation	-.122	.022	-.179**	-.229**
	Sig. (2-tailed)	.051	.728	.004	.000



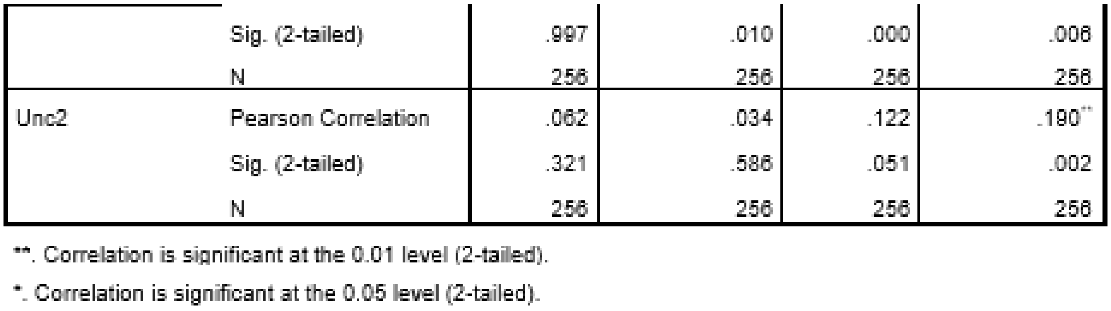
	N	256	256	256	256

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

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

Correlations

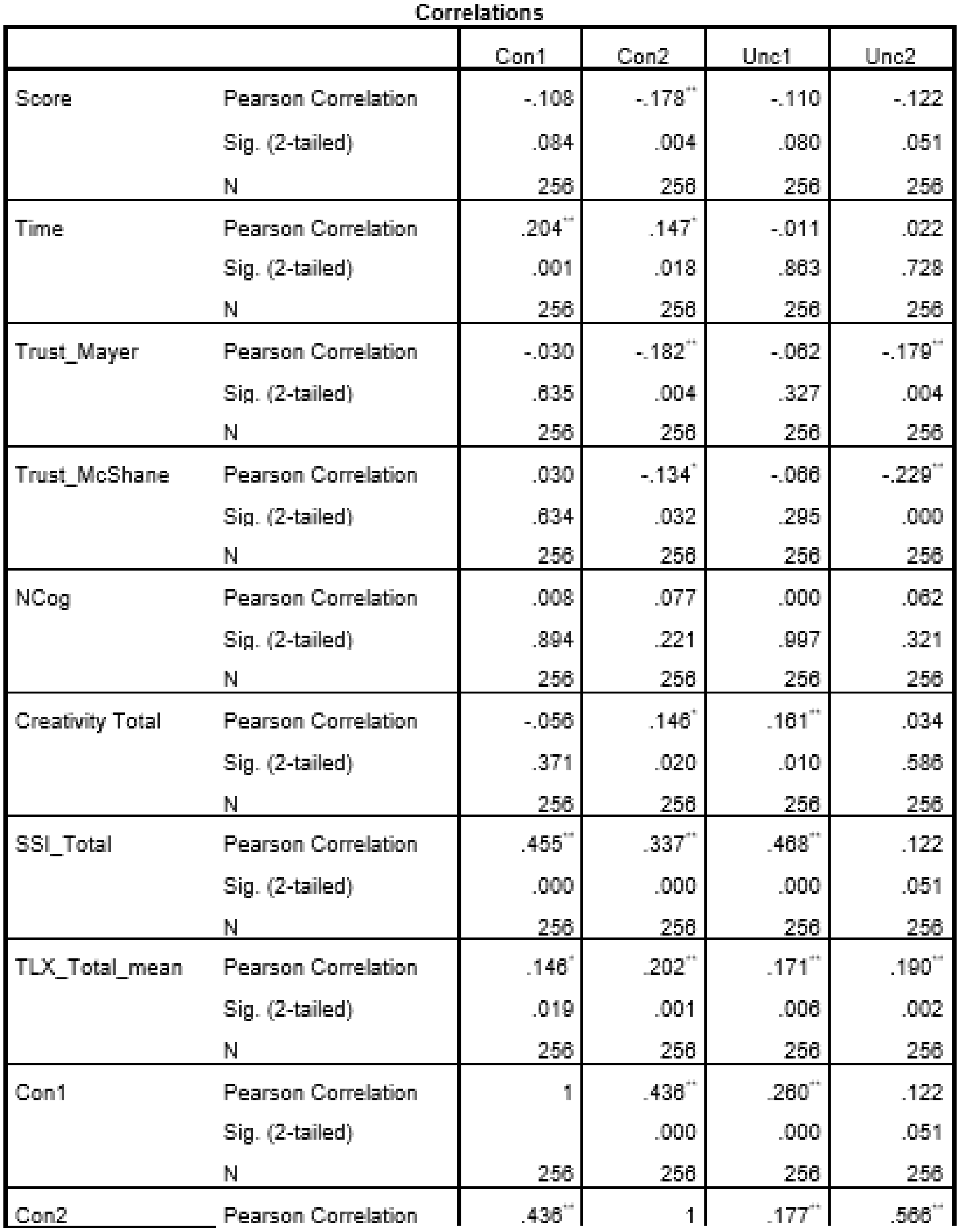
		NCog	Creativity Total	SSI_Total	TLX_Total_mean
Score	Pearson Correlation	-.062	-.102	-.251**	-.188**
	Sig. (2-tailed)	.319	.104	.000	.003
	N	256	256	256	256
Time	Pearson Correlation	.017	.037	.379**	.048
	Sig. (2-tailed)	.783	.560	.000	.448
	N	256	256	256	256
Trust_Mayer	Pearson Correlation	.109	-.213**	-.094	-.089
	Sig. (2-tailed)	.081	.001	.132	.158
	N	256	256	256	256
Trust_McShane	Pearson Correlation	.185**	-.224**	-.143*	-.033
	Sig. (2-tailed)	.003	.000	.022	.602
	N	256	256	256	256
NCog	Pearson Correlation	1	.265**	.105	.101
	Sig. (2-tailed)		.000	.094	.107
	N	256	256	256	256
Creativity Total	Pearson Correlation	.265**	1	.211**	.122
	Sig. (2-tailed)	.000		.001	.052
	N	256	256	256	256
SSI_Total	Pearson Correlation	.105	.211**	1	.335**
	Sig. (2-tailed)	.094	.001		.000
	N	256	256	256	256
TLX_Total_mean	Pearson Correlation	.101	.122	.335**	1
	Sig. (2-tailed)	.107	.052	.000	
	N	256	256	256	256
Con1	Pearson Correlation	.008	-.056	.455**	.146*
	Sig. (2-tailed)	.894	.371	.000	.019
	N	256	256	256	256
Con2	Pearson Correlation	.077	.146*	.337**	.202**
	Sig. (2-tailed)	.221	.020	.000	.001
	N	256	256	256	256
Unc1	Pearson Correlation	.000	.161**	.468**	.171**



	Sig. (2-tailed)	.997	.010	.000	.008
	N	256	256	256	256
Unc2	Pearson Correlation	.062	.034	.122	.190**
	Sig. (2-tailed)	.321	.586	.051	.002
	N	256	256	256	256

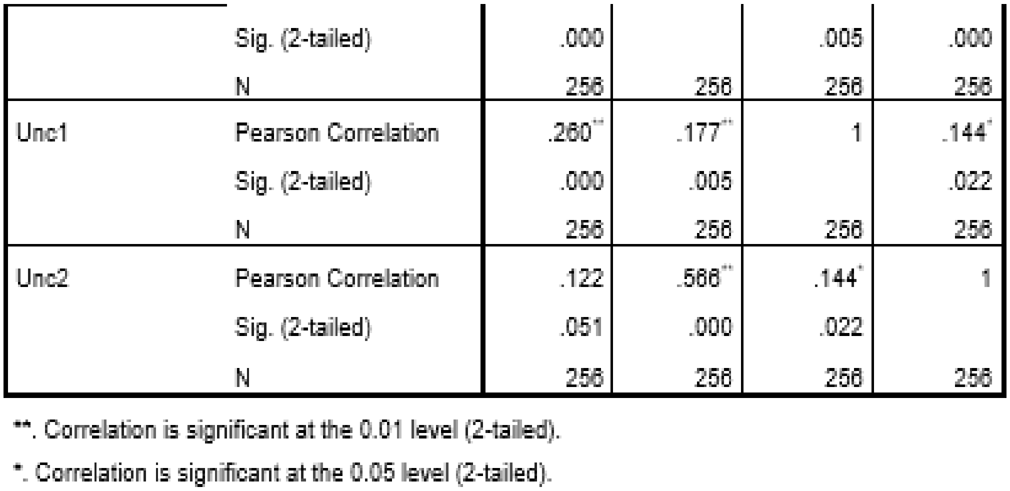
**. Correlation is significant at the 0.01 level (2-tailed).

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



Correlations

		Con1	Con2	Unc1	Unc2
Score	Pearson Correlation	-.108	-.178**	-.110	-.122
	Sig. (2-tailed)	.084	.004	.080	.051
	N	256	256	256	256
Time	Pearson Correlation	.204**	.147*	-.011	.022
	Sig. (2-tailed)	.001	.018	.863	.728
	N	256	256	256	256
Trust_Mayer	Pearson Correlation	-.030	-.182**	-.062	-.179**
	Sig. (2-tailed)	.635	.004	.327	.004
	N	256	256	256	256
Trust_McShane	Pearson Correlation	.030	-.134*	-.066	-.229**
	Sig. (2-tailed)	.634	.032	.295	.000
	N	256	256	256	256
NCog	Pearson Correlation	.008	.077	.000	.062
	Sig. (2-tailed)	.894	.221	.997	.321
	N	256	256	256	256
Creativity Total	Pearson Correlation	-.056	.146*	.161**	.034
	Sig. (2-tailed)	.371	.020	.010	.586
	N	256	256	256	256
SSI_Total	Pearson Correlation	.455**	.337**	.468**	.122
	Sig. (2-tailed)	.000	.000	.000	.051
	N	256	256	256	256
TLX_Total_mean	Pearson Correlation	.146*	.202**	.171**	.190**
	Sig. (2-tailed)	.019	.001	.008	.002
	N	256	256	256	256
Con1	Pearson Correlation	1	.436**	.260**	.122
	Sig. (2-tailed)		.000	.000	.051
	N	256	256	256	256
Con2	Pearson Correlation	.436**	1	.177**	.566**

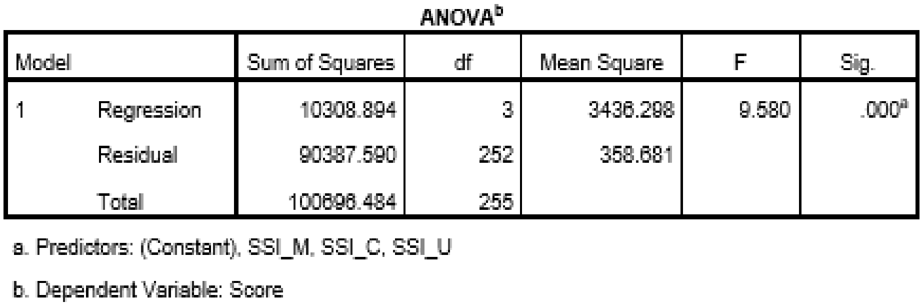


	Sig. (2-tailed)	.000		.005	.000
	N	256	256	256	256
Unc1	Pearson Correlation	.260**	.177**	1	.144*
	Sig. (2-tailed)	.000	.005		.022
	N	256	256	256	256
Unc2	Pearson Correlation	.122	.566**	.144*	1
	Sig. (2-tailed)	.051	.000	.022	
	N	256	256	256	256

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

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

Regression

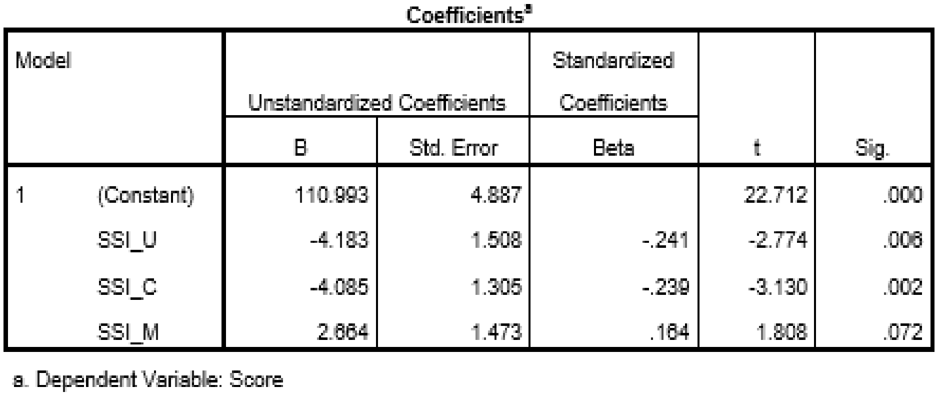


ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	10308.894	3	3436.298	9.580	.000[a]
	Residual	90387.590	252	358.681		
	Total	100696.484	255			

a. Predictors: (Constant), SSI_M, SSI_C, SSI_U

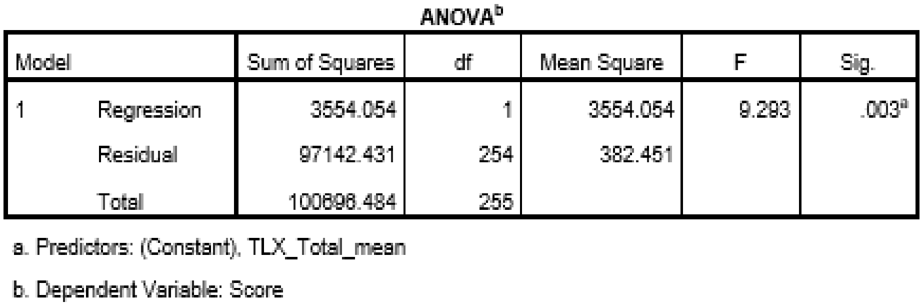
b. Dependent Variable: Score



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	110.993	4.887		22.712	.000
	SSI_U	-4.183	1.508	-.241	-2.774	.006
	SSI_C	-4.085	1.305	-.239	-3.130	.002
	SSI_M	2.664	1.473	.164	1.808	.072

a. Dependent Variable: Score

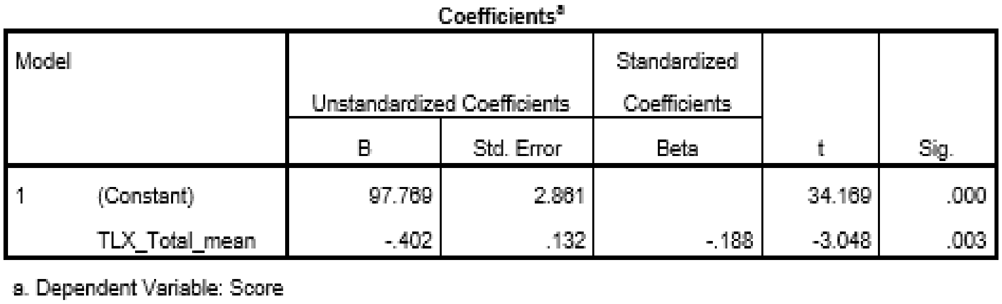


ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	3554.054	1	3554.054	9.293	.003[a]
	Residual	97142.431	254	382.451		
	Total	100696.484	255			

a. Predictors: (Constant), TLX_Total_mean

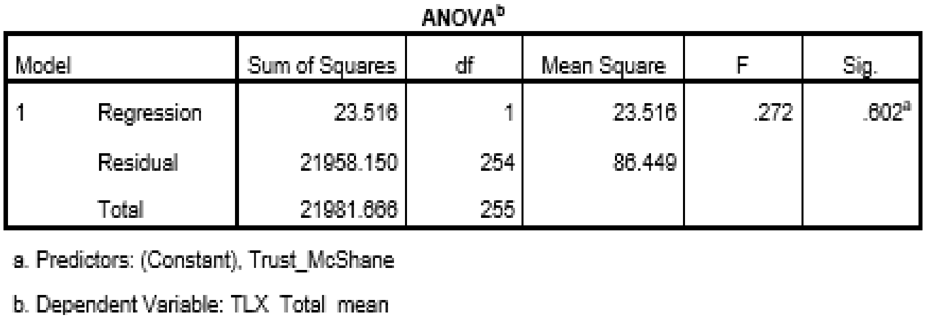
b. Dependent Variable: Score



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	97.769	2.861		34.169	.000
	TLX_Total_mean	-.402	.132	-.188	-3.048	.003

a. Dependent Variable: Score

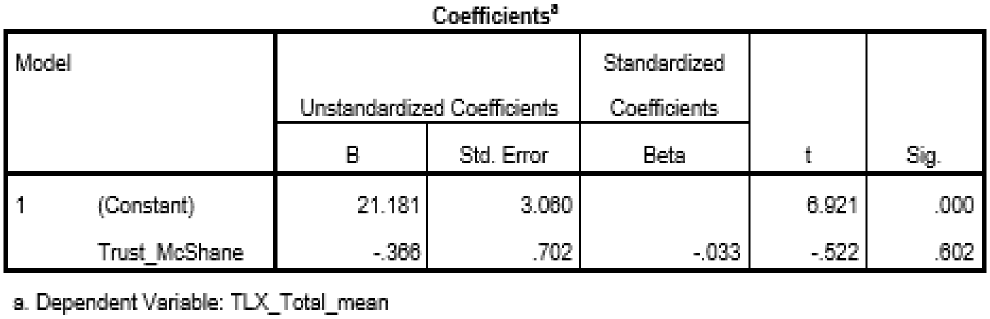


ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	23.516	1	23.516	.272	.602[a]
	Residual	21958.150	254	86.449		
	Total	21981.666	255			

a. Predictors: (Constant), Trust_McShane

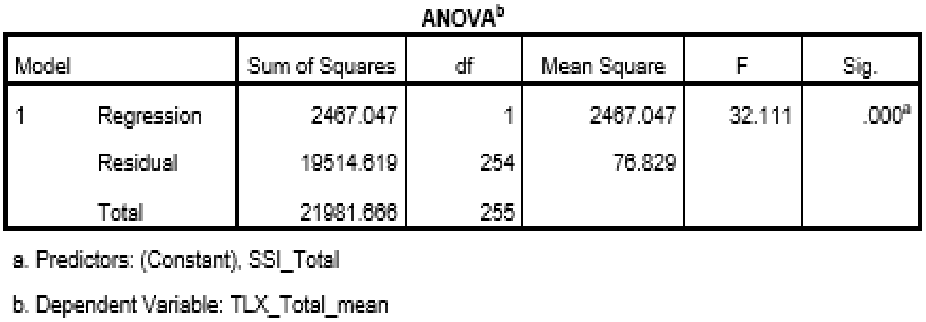
b. Dependent Variable: TLX Total mean



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	21.181	3.060		6.921	.000
	Trust_McShane	-.366	.702	-.033	-.522	.602

a. Dependent Variable: TLX_Total_mean

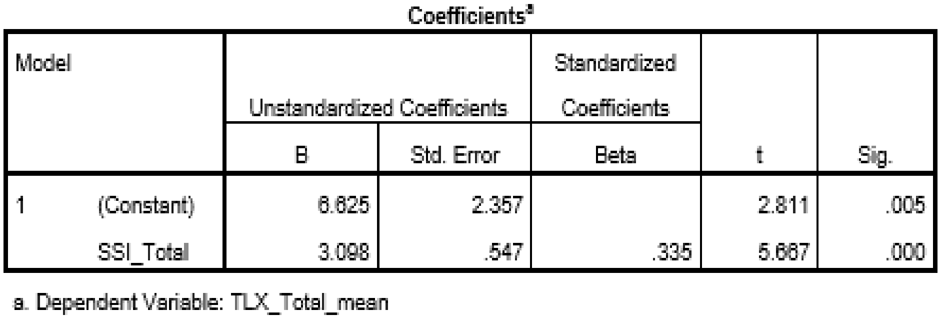


ANOVA[b]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	2467.047	1	2467.047	32.111	.000[a]
	Residual	19514.619	254	76.829		
	Total	21981.666	255			

a. Predictors: (Constant), SSI_Total

b. Dependent Variable: TLX_Total_mean



Coefficients[a]

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	6.625	2.357		2.811	.005
	SSI_Total	3.098	.547	.335	5.667	.000

a. Dependent Variable: TLX_Total_mean

References

Gay, C., Horowitz, B., Elshaw, J., Bobko, P., & Kim, I. (2017). Operator Suspicion and Decision Responses to Cyber-Attacks on Unmanned Ground Vehicle Systems. *Proceedings Of The Human Factors And Ergonomics Society Annual Meeting*, *61*(1), 226-230. doi: 10.1177/1541931213601540

Gay, C., Horowitz, B., Elshaw, J., Bobko, P., & Kim, I. (2019). Operator Suspicion and Human-Machine Team Performance Under Mission Scenarios of Unmanned Ground Vehicle Operation. *IEEE Access*, *7*, 36371-36379. doi: 10.1109/access.2019.2901258

Kwon, C., Liu, W., & Hwang, I. (2014). Analysis and Design of Stealthy Cyber Attacks on Unmanned Aerial Systems. *Journal Of Aerospace Information Systems*, *11*(8), 525-539. doi: 10.2514/1.i010201

Wang, Y., Yan, G., & Zheng, R. (2018). Vulnerability Assessment of Electrical Cyber-Physical Systems against Cyber Attacks. *Applied Sciences*, *8*(5), 768. doi: 10.3390/app8050768

Bobko, P., Barelka, A., & Hirshfield, L. (2013). The Construct of State-Level Suspicion: A Model and Research Agenda for Automated and Information Technology (IT) Contexts. Human Factors: The Journal Of The Human Factors And Ergonomics Society, 56(3), 489-508. doi: 10.1177/0018720813497052

Clarke, R. (2014). The regulation of civilian drones' impacts on behavioral privacy. *Computer Law & Security Review*, *30*(3), 286-305.

Dawson, J., & Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. *Frontiers In Psychology*, *9*(Article 744), 1-12.

Dykstra, J., & Paul, C. (2015). Stress and the Cyber Warrior: Workload in a Computer Operations Center. *Journal of Sensitive Cybersecurity Research and Engineering*, *3*(1), 1-23.

Fan, W., Lwakatare, K., & Rong, R. (2017). Social Engineering: I-E based Model of Human Weakness for Attack and Defense Investigations. *International Journal Of Computer Network And Information Security*, *9*(1), 1-11. doi: 10.5815/ijcnis.2017.01.01

Hirshfield, L., Bobko, P., Barelka, A., Costa, M., Funke, G., & Mancuso, V. et al. (2015). The Role of Human Operators' Suspicion in the Detection of Cyber Attacks. *International Journal Of Cyber Warfare And Terrorism*, *5*(3), 28-44. doi: 10.4018/ijcwt.2015070103

Jamshidi, M., Jaimes Betancourt, A., & Gomez, J. (2011). Cyber-physical control of unmanned aerial vehicles. *Scientia Iranica*, *18*(3), 663-668. doi: 10.1016/j.scient.2011.05.004

Ji, X., Niu, Y., & Shen, L. (2016). Robust Satisficing Decision Making for Unmanned Aerial Vehicle Complex Missions under Severe Uncertainty. *PLOS ONE*, *11*(11), e0166448. doi: 10.1371/journal.pone.0166448

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security*, *38*(2), 7-40.

Kim, A., Wampler, B., Goppert, J., Hwang, I., & Aldridge, H. (2012). Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. *Infotech@Aerospace 2012*. doi:

10.2514/6.2012-2438

King, Z., Henshel, D., Flora, L., Cains, M., Hoffman, B., & Sample, C. (2018). Characterizing and Measuring Maliciousness for Cybersecurity Risk Assessment. *Frontiers In Psychology*, *9*(Article 39), 1-19.

Manesh, M., & Kaabouch, N. (2019). Cyber Attacks on Unmanned Aerial System Networks: Detection, Countermeasure, and Future Research Directions. *Computers & Security*. doi: 10.1016/j.cose.2019.05.003

Moga, H., Boscoianu, M., Ungureanu, D., Sandu, F., & Boboc, R. (2016). Network of Unmanned Systems Cyber Attacks over National Economy Infrastructures. *Applied Mechanics And Materials*, *859*, 144-152. doi: 10.4028/www.scientific.net/amm.859.144

Paganini, P. (2019). Hacking Drones … Overview of the Main Threats. Retrieved from https://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/#gref

Paul, C., & Dykstra, J. (2017). Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations. *Journal of Information Warfare*, *16*(2), 1-11.

Rani, C., Modares, H., Sriram, R., Mikulski, D., & Lewis, F. (2015). Security of unmanned aerial vehicle systems against cyber-physical attacks. *The Journal Of Defense Modeling And Simulation: Applications, Methodology, Technology*, *13*(3), 331-342. doi: 10.1177/1548512915617252

Sedjelmaci, H., Senouci, S., & Messous, M. (2016). How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?. *2016 IEEE Global Communications Conference*

(GLOBECOM). doi: 10.1109/glocom.2016.7841878

Sedjelmaci, H., Senouci, S., & Messous, M. (2016). How to Detect Cyber-Attacks in Unmanned Aerial Vehicles Network?. 2016 IEEE Global Communications Conference (GLOBECOM). doi: 10.1109/glocom.2016.7841878