CYBER SECURITY AND LAW ENFORCEMENT UNMANNED AIRCRAFT SYSTEMS

by

Chasity L. Robinson

A Thesis Presented In Partial Fulfillment
of the Requirements for the Degree of
Master of Science in Aviation Administration

Middle Tennessee State University
December, 2016

Thesis Committee:

Dr. Wendy Beckman, Chair

Dr. Andrea Georgiou

Dedicated in the sweet, loving memory of my grandmother.

She was proud, hopeful, encouraging, and mentoring throughout my life and aspirations.

She always yearned to know how far I was going.

I will keep going on for you, Granny!

ACKNOWLEDGEMENTS

It is with the most sincere gratitude to acknowledge and thank all those who have been a part of my successful completion of the Aerospace Master's program at Middle Tennessee State University. I personally want to recognize my parents and grandfather. They were very supportive and encouraging when I received an acceptance letter from MTSU to finish up my bachelor's degree and continued their support and encouragement when I was accepted into the MTSU's Aerospace Graduate Program. They knew and understood there were times I could not come home to visit, even for holidays, due to homework, tests, papers, and work. They have been extremely patient and loving.

I also would like to recognize my boyfriend, who has been kind and patient throughout this journey. He was there as a listener when I needed to vent out stress. He gave advice and different perspectives on ideas and theories that allowed me to improve my thesis. He encouraged me daily and hugged me when I needed it the most.

Lastly, I would like to personally thank and recognize my Thesis Committee members, Dr. Beckman (Chair) and Dr. Georgiou. They have truly encouraged me to do my best at all times. I have learned so much from them whether it was in the classroom, events, or just some mentoring guidance in their office. They have taken their time out of their busy schedule to meet with me, e-mail or call, and read and revised my thesis along with other past assignments. They are not only helpful and encouraging to me, but they are very helpful and encouraging to other students. This whole journey of mine would not have been complete if it was not for them.

ABSTRACT

Unmanned Aircraft Systems (UAS) have created a universal paradigm shift within political, commercial, military, recreational, and emergency response operations. For example, law enforcement departments have started to utilize UAS due to their operational advantages. However, the continuous development and utilization of UAS have resulted in security concerns. Therefore, the purpose of this study was to examine the cyber security vulnerabilities of UAS and their impact on law enforcement use of UAS. This study utilized a survey based on a likert-scale and a literature analysis to collect data and answered the study's research questions. This study has identified available resources for hackers to successfully collect data from law enforcement UAS. The study revealed that law enforcement do not believe hackers can collect data from law enforcement UAS to pose harm on public safety. However, law enforcement does view cyber hacking on law enforcement UAS as a security risk due to malfunction, inadequate training, unauthorized access, and irresponsible operations.

TABLE OF CONTENTS

LIST OF FIGURES

Figure

CHAPTER I INTRODUCTION

Unmanned Aircraft Systems have created a universal paradigm shift within political, commercial, military, recreational, and emergency response operations. Some Unmanned Aircraft Systems operations include utilizing such technology for hobby purposes, competitions, tracking suspects and vehicles, aiding in search and rescue efforts, detection of hazards, and participating in investigations. These Unmanned Aircraft Systems operations have resulted in privacy and safety concerns. The Federal Aviation Administration (FAA) realizes these concerns and has established current regulations in regards to the purpose and usage of Unmanned Aircraft Systems.

Law enforcement departments have started to utilize Unmanned Aircraft Systems due to their operational advantages. Unmanned Aircraft Systems are capable of capturing aerial footage in confined areas without contaminating the environment. Law enforcement departments also recommend the use of Unmanned Aircraft Systems due to the lesser cost of owning, operating, maintaining, and staffing compared to manned police helicopters (Association for Unmanned Vehicle Systems International [AUVSI], n.d.). Examples of uses for which law enforcement departments value Unmanned Aircraft Systems are: tactical operations, criminal pursuit, traffic management, forensics, border patrol, aerial policeman, crime scene investigations, accident investigations, and disaster response efforts (Homeland Surveillance Electronics [HSE], 2015).

The continuous development and utilization of Unmanned Aircraft Systems expands concerns and issues involving such technology. Therefore, it is essential and relevant to research the security risks such as cyber hacking for Unmanned Aircraft Systems. Research on the topic will assist in evaluating the procedures, usage, and handling of Unmanned Aircraft Systems that obtain pertinent and confidential data.

Literature Review

An aircraft that is controlled and navigated by only a remote-controlled pilot or by an automated system is referred to as Unmanned Aircraft Systems (UAS) or Unmanned Aerial Vehicles (UAV). These devices have also been commonly known as drones (International Association of Fire Chiefs [IAFC], 2014). These devices were first implemented during the First World War (approximately 95 years ago), later developed utilization within the interwar period, and then enhanced the operation of aerial torpedoes and cruise missiles (Keane & Carr, 2013).

The Navy and Air Force observed the potential of the cruise missiles and began to seek a continuation of technological advancements of this type of Unmanned Aircraft System. It was later that Unmanned Aircraft Systems obtained the capability to transmit intelligence, surveillance, and reconnaissance (ISR) data from hostile locations. Unmanned Aircraft Systems were able to retrieve pertinent information that obtained a target's location without jeopardizing lives and causing damage (Keane & Carr, 2013).

ISR data collections with both lethal and nonlethal intentions along with training purposes were the three categories of uses that were utilized during the WWII. However, as these enhancements were developed for Unmanned Aircraft Systems, difficulties also evolved. Stabilization, launch, and recovery issues persisted during the operations of Unmanned Aircraft Systems; this, along with additional weapon system developments and the lack of cost effectiveness, decreased the interest in Unmanned Aircraft Systems operations during the war (Keane & Carr, 2013).

Eventually, new attention was brought to Unmanned Aircraft Systems during the interwar period due to the growth of the aviation industry. The interest was regained because of the capabilities in successfully completing missions without compromising human life and reducing damages and injuries (Tomiuc, 2012). Therefore, as the interest in Unmanned Aircraft Systems continued, so did the progression of enhancements for the unmanned vehicles.

An example of Unmanned Aircraft Systems utilization due to the technological progression and enhancements can be seen by the Central Intelligence Agency (CIA). The CIA first implemented Unmanned Aircraft Systems within the military. The CIA had been operating unarmed Unmanned Aircraft Systems since 2000; however, the CIA began arming their Unmanned Aircraft Systems after the September 11, 2001 attacks. It was later documented that on February 4, 2002, the CIA was the first to utilize an armed Unmanned Aircraft Systems, the Predator, for the targeted killing of Osama Bin Laden in Paktia within Afghanistan (Sifton, 2012).

Unmanned Aircraft Systems utilization has continued to evolve in order to complete various tasks. The unmanned vehicles can detect gases, monitor hazardous situations and other environments without exposing emergency responders or contaminating the scene, aid in search and rescue missions, and search for cleared roadways. Unmanned Aircraft Systems operations also allow the capacity to capture images and videos of areas that have been affected by natural disasters (i.e. hurricanes, tornadoes, fires, sinkholes, floods, and earthquakes).

A specific example for Unmanned Aircraft Systems utilization was after the devastating earthquake that occurred in Ludian, Yunnan, China. Over three thousand people were injured, 114 were reported missing, 617 people were fatally injured, and over a million people were affected by the destruction as a result of the 6.5 magnitude earthquake. Once the earthquake subsided, the China Association for Disaster and Emergency Response Medicine quickly utilized their Unmanned Aircraft Systems to search for cleared roads and survivors and to assess the damage (Vervaeck, 2014; Press, 2014).

The trend of Unmanned Aircraft Systems has developed rapidly internationally and domestically. Although Unmanned Aircraft Systems technology has progressed for various utilizations, unfortunately, uncivilized and unwanted practices have increased as well. Due to the quick growth of Unmanned Aircraft Systems operations, the American Civil Liberties Union expressed concerns about law enforcement UAS operations, while the Federal Aviation Administration (FAA) is concerned about the risk of general Unmanned Aircraft Systems operations. Therefore, the FAA implemented the necessary actions to assist in alleviating and preventing uncivilized and unwanted practices, including any concerns that threaten to violate the Fourth Amendment of the U.S. Constitution (Canis, 2015).

Regulations

Currently, there are three categories of Unmanned Aircraft Systems operations: Model Aircraft Operations, Public Operations, and Civil Operations. Model Aircraft Operations are classified as hobby or recreational uses (i.e. flying in competitions). To promote safety and the proper use for these operations, the Federal Aviation

Administration (FAA) has implemented “Know Before You Fly” Campaigns (Federal Aviation Administration [FAA], 2015c). This campaign illustrates the appropriate responsibilities of owning and flying such technology.

Another category of Unmanned Aircraft Systems is for Governmental purposes (Public Operations). Title 49 U.S.C. 40102(a)(41) and 40125 outlines the specific qualifications operators under Unmanned Aircraft Systems Public Operations should obtain. Each Governmental task for Unmanned Aircraft Systems is verified on a flight-by-flight basis, which considers the operator, ownership of the Unmanned Aircraft Systems, and the purpose of the flight (Federal Aviation Administration [FAA], 2015a). For agencies implementing Unmanned Aircraft Systems in a particular area and for a particular purpose, a Certificate of Waiver or Certificate of Authorization (COA) must be obtained. The FAA distributes the COA, which allows organizations and agencies to operate their Unmanned Aircraft Systems (FAA, 2015a).

The third category of UAS operations is for Non-Governmental purposes (Civil Operations). Civil Operations are classified as such when “operations do not meet statutory criteria for public aircraft operations” (Federal Aviation Administration [FAA], 2015b, para. 1). Although the FAA requires that Unmanned Aircraft Systems operating Non-Governmental purposes must follow the Code of Federal Regulations, these operations must also obtain a Section 333 Exemption and Special Airworthiness Certificate (SAC). This allows the Unmanned Aircraft Systems operator to submit a detailed description of how their UAS was manufactured, designed, constructed, the procedures utilized, and the purpose and duration of the flight (FAA, 2015b).

The FAA has also developed and implemented a registration system for Unmanned Aircraft Systems for the operations of public, commercial, and non-model aircraft. This process is web-based and requires any Unmanned Aircraft Systems weighing more than 0.55 pounds but less than 55 pounds to register their device. Owners must be 13 years of age or older and a legal permanent resident or U.S. citizen; however, if the owner is less than 13 years old then a person who is 13 years old or older must register the unmanned aircraft. If the Unmanned Aircraft Systems weighs more than 55 pounds, will operate internationally from the U.S., is owned by a trustee, or the owner utilizes a voting trust to satisfy the U.S. citizen requirements, then the owner must undergo the Aircraft Registry process, which is paper-based. It is also important to acknowledge that registration is a requirement in order for owners who operate under a Section 333 exemption (Federal Aviation Administration [FAA], 2016).

If any owner fails to register their Unmanned Aircraft Systems, then civil penalties of $27,000 maximum, criminal fines of $250,000, and a maximum of three years of imprisonment will be distributed accordingly. The Unmanned Aircraft Systems registration process will assist in ensuring safe practices for operators, manned aircraft, and other surrounding people and objects. Registration of Unmanned Aircraft Systems will also allow for the devices to be traceable during an incident (FAA, 2016).

In order to continue safe Unmanned Aircraft Systems operations, especially in and around airports and other critical infrastructures, the FAA has implemented a Pathfinder Program. The Pathfinder Program allows detection and identification of Unmanned Aircraft Systems that are airborne too close to airports or any other significant buildings. The FAA has signed CRDA's (Cooperative Research and Development

Agreements) with Sensofusion, Liteye Systems Inc., and Gryphon Sensors. These agreements will allow the FAA to evaluate various technologies and procedures in detecting, tracking, and identifying unauthorized Unmanned Aircraft Systems within and around airports and sensitive areas (FAA, 2016).

This software-based technology was first implemented within three European armies as a military project in order to locate, track, and access control over Unmanned Aircraft Systems. The technology was known and described as an “AIRFENCE,” which protected military areas, government buildings, police, and prisons within Europe. Since the popularity of Unmanned Aircraft Systems is increasing, it is essential to implement such technology to safely integrate Unmanned Aircraft Systems operations. This will also allow the Unmanned Aircraft Systems operators to continue and safely execute their mission, but prevent unlawful actions by others who desire harm (FAA, 2016).

It appears Unmanned Aircraft Systems purposes are expanding within each Unmanned Aircraft Systems category and progressing in their overall effectiveness with daily tasks. For example, law enforcement agencies utilize UAS for border control, hostage crisis, accident investigations, disaster relief efforts, criminal pursuit, aerial policemen, GPS and mapping applications, traffic management, crime scenes, tactical operations, forensics, chemical, biological, radioactive, nuclear, and explosives operations (HSE, 2015; Connor, 2015). More specifically, a police department in Canada utilized an unmanned aircraft system to help save a human life. In May 2013, the Royal Canadian Mounted Police utilized their Draganflyer X4-ES to locate a person who had been in a vehicle accident and suffered a head injury. The injured person had unknowingly walked away from the scene during subfreezing temperatures. It was vital that the responders locate the disoriented individual quickly considering the victim had sustained injuries and it was during the subfreezing night, to prevent worsened injuries. The Royal Canadian Mounted Police had equipped a helicopter with night-vision technology, along with a crew on the ground, to search for the individual but had failed to locate them. The police decided to utilize their unmanned aircraft, which contained a Forward Looking Infrared (FLIR) camera. The device was successful in locating the injured individual (Connor, 2015).

Another instance that an unmanned aircraft was utilized during law enforcement response was in Nova Scotia, Canada. Law enforcement utilized their unmanned device to locate a family that was lost in the woods (Connor, 2015). Unmanned Aircraft Systems utilize an optical instrument that operates as a transit or electronic theodolite that obtains an electronic distance meter, which is used for surveying. This gathers slope distances information from a particular point (i.e. curve of a street). This type of technology can be utilized by law enforcement during a police chase or a shooting crime scene. Law enforcement can fly an unmanned aircraft system to survey and search the scene route to look for evidence (Dunn, 2014). Unmanned aircraft systems can reconstruct a crime scene and turn aerial photos into a three-dimensional model for investigative purposes (Greene, 2013).

Cyber Hacking

Although unmanned aircraft systems have operational advantages, it is also pertinent to understand the risks of such devices, such as cyber hacking. In December 2012, the Iranian government seized United States CIA’s Lockheed Martin RQ-170 Unmanned Aircraft System. The Unmanned Aircraft System was utilized in gathering intelligence. The Unmanned Aircraft System was captured near the Iran-Afghanistan border. The Iranian government appeared to study the components including mission data and analyzed maintenance logs of the Unmanned Aircraft Systems. The Iranian government was able to acquire access to the unmanned device's historical data, including sensitive information of ongoing missions (Paganini, 2013; Moskvitch, 2014).

Another cyber security hacking instance occurred with a civilian Unmanned Aircraft Systems. In December 2013, Sammy Kamkar, an independent IT security analyst, hacked and controlled a Parrot AR Drone 2.0. He was able to successfully complete the hack by equipping the Unmanned Aircraft Systems with a small Raspberry Pi computer, two wireless transmitters, and a battery. He was able to initiate the hack with software equipped on the small computer, which allowed the Unmanned Aircraft Systems to be captured through Wi-Fi signals (Moskvitch, 2014).

As mentioned previously, there are more developments in the Unmanned Aircraft Systems industry; however, as these developments are being implemented, more issues and concerns are raised. For example, ensuring that the devices are secured by encryption along with procedures to determine and diagnose the results of a cyber attack is problematic within these systems (Bunker, 2015). Therefore, it is essential to analyze the potential hazards with such devices and develop tactics to overcome these issues.

Before examining the potential cyber-security hazards of UAS along with researching preventive measures for those hazards, it is imperative to acknowledge the history of cyber-security. Since the development of the ARPANET (Internet's predecessor) in the 1980's, cyber-security issues have evolved. However, the severity and impact of cyber-security attacks have continued to increase. In 1989, computers were infected with the “Morris Worm.” This was the first virus to infect and affect computers, and closed down most of the Internet. Robert Morris was responsible for creating the rapid and aggressive virus, which provided a denial-of-service (DoS) attack (Julian, 2014). The virus occurred due to a programming error in a project that was to determine the Internet’s size by infecting its UNIX systems. This was supposed to allow the existing number of connections to be counted in order to determine the size of the Internet; however, the programming error occurred and caused system crashes and clogged networks. Therefore, computers that were infected became unusable. This led to the development of the Computer Emergency Response Teams (CERTs) (Julian, 2014; NATO, n.d.; Press, 2015).

The next significant viruses that affected computers occurred in the late 1990’s and early 2000’s. Tens of millions of computers were infected by the “Melissa” and “ILOVEYOU” viruses that were distributed through email accounts. The viruses affected email accounts worldwide by persuading recipients with a financial or other motive to open the infected email. This incident provided more awareness for users to be cautious when accessing emails and opening attachments from unknown and distrusted sources. The antivirus was developed and implemented to prevent these types of viruses. This technology allowed for the signature of a virus to be recognized and prevent the virus from executing (Julian, 2014).

Between 2005 and 2007, another security breach occurred. Albert Gonzalez stole information from approximately 45.7 million credit card payments that belonged to TJ Maxx customers. The authorities had to be involved extensively due to the confidential data that was stolen from the customers’ credit card payments and each customer had to be compensated. This breach cost the company $256 million and the company suffered from the consequences of not acquiring a secure system. A similar breach occurred in 2013 when cyber attacks struck customers' credit and debit cards at Target. The breach affected 40 million credit and debit cards by accessing the information through a third party to Target. The cyber attack retrieved the card numbers by utilizing a specific code for the point-of-sale (PoS) systems when the numbers in the system were not encrypted. After the incident, many organizations, including Target, understood the importance of establishing the appropriate preventive breach resources, detecting if and when breaches occur, and responding appropriately and quickly to the incident (Julian, 2014).

According to NATO (n.d.), cyber attacks have occurred at least once annually in 2006 through 2012. For example, in 2007, the email account of U.S. Secretary of Defense was hacked by a foreign trespasser. This was part of sequence of attacks in order to gain access to the Pentagon's networks. Another cyber attack incident occurred in July 2011 when a defense contractor was hacked and resulted in 24,000 files stolen from the Department of Defense. A worldwide cyber attack was discovered in October 2012. Kaspersky, a Russian organization, discerned that the attack had been functioning since 2007. The attack was known as "Red October" and had affected the former USSR, Central Asia, Eastern and Western Europe, and North America. Information was gathered from Microsoft's Excel and Word and programs due to vulnerabilities in those systems. The virus retrieved information from energy providers, nuclear and other significant infrastructures, research organizations, government embassies, and military installations (NATO, n.d.).

As technology develops, cyber-security vulnerability concerns increase as well. The demands in the importance of understanding cyber-security vulnerabilities, along with preventive procedures against attacks, must be established. Former U.S. Secretary of Defense, Leon Panetta, expressed that a cyber attack can be as destructive and devastating as the September 11, 2001 terrorist attacks if extremist groups or other nation states discover and access cyber vulnerabilities (NATO, n.d.).

To better understand the cyber risks against technological advancements such as Unmanned Aircraft Systems, it is essential to recognize that Unmanned Aircraft Systems are equipped with different systems and various components that can be targeted from cyber attacks. Unmanned Aircraft Systems basic elements involve propellers, frame, battery and motor, Global Positioning Systems (GPS), electronic sensors, and some are equipped with a camera, radio and Wi-Fi receivers. Unmanned Aircraft Systems can be operated by either a tablet, smartphone, or by controllers. Even though some Unmanned Aircraft Systems acquire gasoline motors to operate, typically smaller Unmanned Aircraft Systems utilize electric motors. These unmanned devices extract energy either from fuel cells, solar cells, or batteries then achieve lift from the horizontal propellers (Canis, 2015).

More specifically, the more complex components that are found in Unmanned Aircraft Systems include the airspeed or altimeter, main program or processor, wireless communication, GPS, magnetometer, Inertial Measurement Unit, power system, actuators, manual flight control, boot loader reset switch, and data links. The airspeed or altimeter component is designed to measure the altitude and airspeed of the Unmanned Aircraft Systems. Then the main program processes the sensor data and the control implementation of the unmanned device while communications with the ground station is conducted by the wireless communication. The global position of the unmanned aircraft is determined by the GPS, but the direction is measured by the magnetometer, which receives information from other sensors on the Unmanned Aircraft Systems (Kim, Wampler, Goppert, Hwang, & Aldridge, 2011; Rivera, Baykov, & Gu, n.d.).

However, the Inertial Measurement Unit is utilized to measure Unmanned Aircraft Systems movement, while the power system provides power to the device. Then the unmanned device moves its control surfaces by receiving commands from the main processing board (actuators). The actuators receive input from sensors, along with the preloaded and current Unmanned Aircraft Systems commands. This determines the navigation for the Unmanned Aircraft Systems. The autopilot is overridden and initiates control of the Unmanned Aircraft Systems control surfaces to the ground station by the manual flight control and lastly, programs are loaded within the main program board by the boot loader reset switch. The data links, which are part of the communication systems, consists of modems, Radio Frequency transmitter, receiver, and an antenna. The data links uplink from a satellite or ground station in order to send control data to Unmanned Aircraft Systems. The data links also downlink from the unmanned device to send data from the telemetry system and onboard sensors to the ground station and it measures range and azimuth from the satellite and ground station to the Unmanned Aircraft Systems in order to attain successful communication between them (Kim et al, 2011; Rivera et al, n.d.; Gupta, Ghonge, & Jawandhiya, 2013).

Access of these vehicles can be gained and controlled against the operator by a remote attacker. These systems are desirable to hack due to pertinent and confidential data acquired. In the perspective of the military, information that is obtained can include images, location of troops, items or persons of interest, and other sensitive information (Paganini, 2013). This remains a great concern for both military and civilian purposes of Unmanned Aircraft Systems due to GPS spoofing and jamming, cyber espionage, malware-based attacks, and network exploits to extract industrial secrets and harm against public safety (Paganini, 2012).

Global Positioning System (GPS) spoofing occurs when fictitious geographical coordinates are sent to the unmanned vehicle, causing it to be deceived and travel to a different location at a different time, when the device believes it is traveling to the original location it was set to locate to at its predicted time. This type of an attack can occur due to the GPS's encrypted signal use being leaked. Hackers (or "spoofers") can capture and control Unmanned Aircraft Systems by utilizing its GPS, and then they can cause it to locate toward a different area or specifically collide into a targeted area (Paganini, 2013).

GPS signal jamming is another cyber security method that can be completed by unauthorized personnel. Jamming the signals to GPS causes the transmissions that are being received by the GPS to be interrupted. Thus, the Unmanned Aircraft Systems loses the ability to monitor routes and calculate the location, direction, and altitude of its flight path. In other words, all communications of information sent to the Unmanned Aircraft Systems is blocked. Once the signals are jammed, the Unmanned Aircraft Systems will crash. This is a concern because the Unmanned Aircraft Systems can collide into objects (i.e. power lines, buildings, vehicles, traffic, et al) and people creating serious damages and injuries (Paganini, 2013).

Another cyber security concern for Unmanned Aircraft Systems are cyber attacks that are malware-based. Malware-based attacks involve a malicious code that infects the Unmanned Aircraft Systems (sending a virus). These types of attacks exploit the vulnerabilities that evade security-related controls and strike the vehicle device. These unmanned vehicles are comprised of diverse components, which appear attractive for an attacker to seek out vulnerabilities within each component system in order to control the overall vehicle (Paganini, 2013).

Lastly, cyber espionage is a vital concern to acknowledge in order to prevent such attacks. Cyber espionage is the utilization of stealing and collecting information (also known as spear-phising) (Paganini, 2013). Other cyber security-related vulnerabilities of Unmanned Aircraft Systems are interrupting and capturing the data links from the unmanned devices. This includes access to what the Unmanned Aircraft Systems is looking at, especially if the data is not encrypted (Paganini, 2012).

As previously mentioned, law enforcement departments have gained interest in the utilization of unmanned aircraft systems due to operational advantages. However, there are concerns of hacking such devices due to cyber espionage, malware-based attacks, GPS spoofing and jamming, and network exploits. According to David Mascarenas, from National Security Eduction Center, Unmanned Aircraft Systems are "flying computers" and have the potential to reveal security flaws (Moskvitch, 2014). These unmanned devices also have the potential of being controlled along with confidential data accessed by an attacker; therefore, it is necessary to investigate cyber security vulnerabilities of law enforcement Unmanned Aircraft Systems. Research of this topic should also include recommendations, solutions, and preventive measures against cyber hacking. More specifically, the research topic and research questions are listed below.

Research Topic and Research Questions

The purpose of this study is to examine the cyber security vulnerabilities of Unmanned Aircraft Systems and their impact on Law Enforcement use of Unmanned Aircraft Systems. This study will specifically focus on answering the following research questions:

1. Based on literature analysis, what resources do hackers have that would allow them to successfully collect confidential data from Law Enforcement Unmanned Aircraft Systems?
2. Do Law Enforcement Officers believe hackers can collect data from Law Enforcement Unmanned Aircraft Systems to pose harm on public safety, and if so, what are those public safety concerns?
3. Do Law Enforcement officials view cyber hacking on Law Enforcement Unmanned Aircraft Systems as a security risk, and what are these security risk concerns?

CHAPTER II METHODOLOGY

In order to determine cyber security vulnerabilities of law enforcement unmanned aircraft systems, a qualitative research method was pursued. Data was collected from an anonymous survey that was distributed via SurveyMonkey, and additional information was collected and compiled via a literature analysis. The survey methodology was the most appropriate for this study as this seemed to be the best approach to determine the current opinions of law enforcement officers, or those who assist law enforcement officers. The survey was utilized to determine what data law enforcement officers believe hackers can collect on their unmanned aircraft systems to pose harm on public safety, what those public safety concerns are, if law enforcement officials view cyber hacking on law enforcement unmanned aircraft systems as a security risk, and what those security risk concerns are. A literature analysis was also needed to supplement this study, because it was possible that the answers to the above research questions were better found in literature research than from law enforcement opinions. The literature analysis distinguished resources that are available to hackers that would allow them to successfully collect confidential data from law enforcement unmanned aircraft systems. A combination of both the survey and literature review methodologies was seen as the most effective approach to the study. The research study was granted Institutional Review Board (IRB) approval from Middle Tennessee State University (MTSU) under IRB #007 (see Appendix A).

Participants

The participants were recruited through e-mail correspondence from contact information that was provided by the Association for Unmanned Vehicle Systems International's (AUVSI) Member Directory. Participants were contacted based on 1) their law enforcement experience with Unmanned Aircraft Systems, 2) law enforcement without Unmanned Aircraft Systems experience but having expertise on Unmanned Aircraft Systems, and 3) other departments who assist law enforcement departments with Unmanned Aircraft Systems. Their career and background experience with UAS were identified by their profile on the AUVSI's Member Directory and these individuals were then contacted by e-mail correspondence.

AUVSI's members that responded to the e-mail consented to partake in the research study and also provided additional contacts that would be willing to partake in the study. E-mails that were sent to participants included the informed consent regarding the research study. Eleven participants agreed to complete the survey. These participants included former or current members of the Arlington Police Department in Texas, Montgomery County Sheriff's Office in Texas, Frisco Texas Fire Department in Texas, Mesa County Sheriff's Office in Colorado, Miami-Dade Police Department in Florida, Port St. Lucie Department in Florida, Metropolitan Nashville Airport Authority's Department of Public Safety in Tennessee, New York City Police Department in New York, Ventura Police Department in California, Glendale Police Department Air Support Unit in California, Federal Aviation Administration's Unmanned Aircraft Systems Program Office, and Airborne Law Enforcement Association.

Instruments

The instrument that was utilized was a survey based on the Likert Scale, along with a literature analysis. The survey asked a series of questions about Unmanned Aircraft Systems that are used within law enforcement departments and potential cyber security concerns. The survey questions and the literature analysis was utilized in order to answer the research questions: 1) Based on literature analysis, what resources do hackers have that would allow them to successfully collect confidential data from Law Enforcement Unmanned Aircraft Systems? 2) Do Law Enforcement Officers believe hackers can collect data from Law Enforcement Unmanned Aircraft Systems to pose harm on public safety, and what are those public safety concerns? 3) Do Law Enforcement officials view cyber hacking on Law Enforcement Unmanned Aircraft Systems as a security risk, and what are these security risk concerns?

Data collection for the first research question was addressed by a literature analysis in order to distinguish resources that hackers may have access to that would allow them to collect confidential data from law enforcement unmanned aircraft systems. It is pertinent to understand any technology that is available to hackers in order to research and present resolutions to these issues. The second and third research questions were answered by the survey that was distributed through SurveyMonkey. This survey allowed participants to share their views on cyber security trends and concerns for Unmanned Aircraft Systems. This was important because these individuals are uniquely qualified to address the cyber security vulnerabilities and present solutions for these issues.

Again, the survey questions were designed to answer research questions number two and three (refer to Appendix B for the full text of the survey). More specifically, survey questions numbered 1-7 gathered background information on the topic. It is essential to gather background information from the participants in order to successfully understand the data. Background information contained information regarding the participants' years of experience with a law enforcement department, whether or not that Department utilizes Unmanned Aircraft Systems, how often the Department utilizes Unmanned Aircraft Systems, whether or not the participant are involved with the Department's Unmanned Aircraft Systems Department, total training and total operational experience the participant received for Unmanned Aircraft Systems, and the level of FAA training the participant possesses. Answers from these questions were categorized in order to determine any trends based on security concerns with Unmanned Aircraft Systems. For example, as participants acquire more operational experience, thus gaining more knowledge about Unmanned Aircraft Systems, do they have an increased belief that Unmanned Aircraft Systems are more of a security threat versus participants who have less operational experience?

The second research question, "Do Law Enforcement Officers believe hackers can collect data from Law Enforcement Unmanned Aircraft Systems to pose harm on public safety, and what are those public safety concerns," were answered through survey questions numbered 8-13. Question 8, "How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement Department or the Law Enforcement Department you assist with?" contributed to answering the second research by distinguishing if the Unmanned Aircraft Systems are being effectively utilized or if the unmanned devices are effective. If the unmanned aircraft are ineffective in completing a task, it may establish security concerns. For example, if participants believe Unmanned Aircraft Systems are ineffective at completing tasks then this may be due to insecure features on the devices, which may result in unsuccessful completed missions, which may present other cyber security vulnerabilities.

Questions 9 and 10, "Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are" and "Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?" also assisted in answering the second research question. The data and video links are important components on Unmanned Aircraft Systems. These components allow law enforcement officers to collect data (i.e. video or images) of scenes. This data is essential for successful completed missions and such data should remain confidential for only authorized personnel. Therefore, it is essential to know whether or not these features are secured.

To assist in answering research question 2, survey questions 11 and 12, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during operational use" and "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think a person can hack into Unmanned Aircraft Systems during non-operational use?" were asked. It is essential to distinguish whether or not law enforcement officers and those who assist with law enforcement departments believe that Unmanned Aircraft Systems can be hacked during operational and non-operational uses. If law enforcement departments believe that these devices can be hacked, then other preventive cyber hacking measures should be established and implemented to protect missions and prevent confidential data from being stolen. Lastly, question 13, "How likely do you think it is for a person who hacks into an Unmanned Aircraft Systems to pose harm for public?" assisted in answering research question 2. It is not only important to distinguish whether or not Unmanned Aircraft Systems can be hacked during operational and non-operational use, but also essential to establish if hacked Unmanned Aircraft Systems pose harm for public safety. This question evaluated whether or not law enforcement considers harming public safety with hacked Unmanned Aircraft System as a threat. If there is a concern, then it is essential to establish and implement preventive measures.

The third research question, "Do Law Enforcement Officials view cyber hacking on Law Enforcement Unmanned Aircraft Systems as a security risk, and what are these security risk concerns," was answered through survey questions numbered 13-15. Again, question 13 distinguished if hacked Unmanned Aircraft Systems poses harm for public safety. If law enforcement believes Unmanned Aircraft Systems can be hacked and utilized against public safety, then it will be established that law enforcement views cyber hacking on Unmanned Aircraft Systems as a security risk. Therefore, if there are cyber security risk concerns for Unmanned Aircraft Systems then it is essential to recognize all the possible security risk concerns and establish and implement preventive cyber hacking measures, which was answered by the open-ended survey questions 14 and 15.

Procedures

After the IRB permission was granted, a list of law enforcement departments within the United States that utilized unmanned aircraft systems were compiled as described in the participant section above. The list of the law enforcement departments were contacted via e-mail to gather information on their utilization of unmanned aircraft system and asked if they would be willing to participate in a research study on cyber security vulnerabilities of law enforcement unmanned aircraft systems. Some of the departments did not respond to initial e-mails; however, other departments responded agreeing they would assist in the study. One participant suggested utilizing the AUVSI's Member Directory for additional contacts.

Therefore, members from AUVSI who were law enforcement officers, assisted with Unmanned Aircraft Systems law enforcement departments, or those who assisted in Unmanned Aircraft Systems operations were contacted via e-mail correspondence. Once participants were gathered, the survey was sent to the participants and they were given approximately three weeks to complete the survey.

However, complications arose both before and during the survey. Participants were originally only supposed to be selected based on law enforcement departments who utilize unmanned aircraft systems. Considering the unmanned aircraft systems developments are increasing and regulations of the UAS are being developed and implemented, there are several law enforcement departments waiting for the appropriate COA in order to operate or purchase an UAS. Therefore, some AUVSI members suggested personnel who assist law enforcement departments with UAS in order to gather more participants. That suggestion was considered and both law enforcement departments who utilized unmanned aircraft systems and those who assist law enforcement that utilize unmanned aircraft systems were utilized.

After the survey was completed, research for the literature review and literature analysis was conducted. Research was conducted by searching the Google database, along with MTSU Library's JEWL search engine and the Academic Search Premier database for relevant topics on cyber security on Unmanned Aircraft Systems. Keywords that were utilized within the search included: cyber security, UAS, unmanned aircraft systems, cyber security and unmanned aircraft systems, hacking, hacking UAS, law enforcement unmanned aircraft systems, components of UAS, and systems of UAS. These keywords were most appropriate in order to search the appropriate topic relevant to the research. Approximately 30 articles were found from both the databases and search engine mentioned previously. Approximately 10 of those resources were specifically utilized for data collection. These resources included Kerns, Shepard, Bhatti, & Humphreys (2014), Gupta, Ghonge, & Jawandhiya (2013), Rodday (2015), Kim, Wampler, Goppert, Hwang, & Aldridge (2011), and Rivera, Baykov, & Gu (n.d.), which were found on the MTSU Library's JEWL search engine and Academic Search Premier database. Other resources that were utilized for data collection included Moskvitch (2014), Carr (n.d.), Mendez (2014), Schwartz (2012), and Sneiderman (2016), which were found within the Google search engine. These resources were specifically selected for data collection due to the topic relevancy for the current research topic. These resources provided information in order to compare studies that have been completed. The resources were chosen over other resources due to the information that was utilized to assist in this study and that other topics did not provide the necessary information that was needed. The remaining resources were utilized for gathering background information on the research topic. However, there were other resources that were discovered but were not utilized for the study because of repetitive information, lack of information, or information that was irrelevant to the topic.

CHAPTER III RESULTS

A total of eleven participants from various departments participated in the anonymous survey that was based on a Likert-scale. Each question that was asked to assist in determining any trends that linked cyber security concerns with Unmanned Aircraft Systems for law enforcement departments. The first survey question, "Approximately how long have you been working in Law Enforcement or assisting with Law Enforcement" distinguished any differences in the participants' answers based upon their experience. The answer choices provided were "less than 2 years, 2-5 years, 6-10 years, 11-15 years, 16-20 years, 21-24 years, and more than 25 years." There were no recorded answers for the "less than 2 years" and "2-5 years" choices. However, one participant (9%) categorized themselves as having 6-10 years of experience, two participants (18%) classified as acquiring 11-15 years of experience, one participant (9%) with 16-20 years, one participant (9%) with 21-24 years of experience, and six participants (55%) with more than 25 years of experience (see Figure 1). Results from survey question one indicates that the majority of participants who took the survey had acquired more than 25 years of experience and knowledge, either by assisting a law enforcement department or while employed as a law enforcement officer. This question is essential to acknowledge because it can be assessed that if the participants obtain more experience in their field (law enforcement) then they will acquire more knowledge on the research topic.

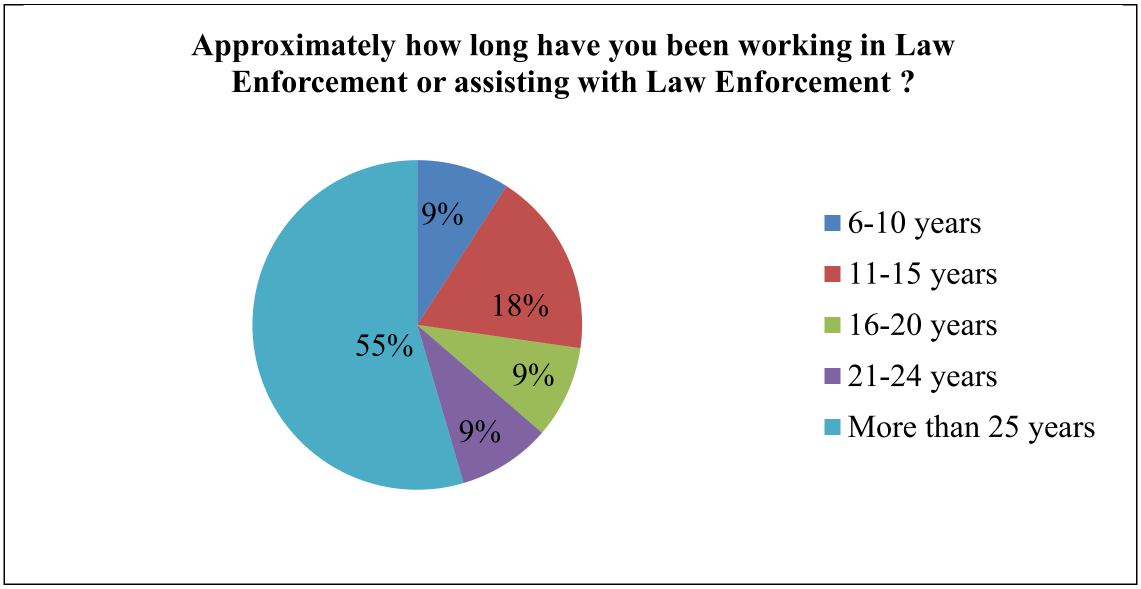


Figure 1. Length of time in Law Enforcement

In order to answer the research questions, more background information was needed from the participants. Question two of the survey asked, “Does your Law Enforcement Department utilize Unmanned Aircraft Systems or does the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems?” The choice selections were “yes” or “no.” Approximately, seven of the participants (64%) answered yes, while the other remaining four participants (36%) answered no. This question is pertinent because it had to be known whether or not the participants are involved with law enforcement departments that utilize unmanned aircraft systems. It was important to acquire participants who have knowledge or experience with unmanned aircraft systems considering the study conducted was on cyber security vulnerabilities with law enforcement unmanned aircraft systems.

The next item that was asked was how often Unmanned Aircraft Systems are used within the law enforcement departments. Survey question three asked, “How often does your Law Enforcement Department or the Law Enforcement Department you assist utilize Unmanned Aircraft Systems?" The options included "once per month, twice per month, once per week, 2-3 times per week, more than 4 times per week, or not sure." Two participants (18%) answered once per month and three participants (27%) twice per month, while six participants (55%) answered "not sure." This question was asked in order to identify how many times throughout each month or week Unmanned Aircraft Systems are being utilized within law enforcement departments. This is essential to know because trends may be identified. Trends such as cyber security vulnerabilities may affect the utilization of the unmanned devices. However, considering 55% of the participants answered "not sure," it is undetermined what caused that answer selection. Perhaps the question did not clearly state the objective or the "not sure" selection was indistinct. There may have not been a particular answer choice available for selection (i.e. does not utilize the Unmanned Aircraft Systems in the law enforcement department due to various reasoning), the participants may not be involved greatly with Unmanned Aircraft Systems operations, or the participants may have not known the total operation usage of Unmanned Aircraft Systems within the law enforcement department.

Question four, "Have you been involved or assisted in a Law Enforcement Unmanned Aircraft Systems Department?" was asked in order to also gather more background information from the participants. There were two options: "yes" or "no." The option "yes" acquired seven participants (64%) while the remaining four participants (36%) answered "no." This provided details that the majority of the participants (64%) were associated with a department which utilized unmanned aircraft systems (referencing back to question one) and that the same number of participants (64%) are also physically involved or assisted with unmanned aircraft systems in that department. This is essential to recognize in order to ensure that the participants are involved with Unmanned Aircraft Systems in a law enforcement department considering the topic of the research.

After establishing how many of the participants were involved with Unmanned Aircraft Systems within a law enforcement department, it was important to determine how much training was received for Unmanned Aircraft Systems. Unfortunately, only eight of the eleven participants answered the question, "How much total training have you received for Unmanned Aircraft Systems operations?" The answer selections were "less than a week, 1-3 weeks, 4-7 weeks, 8-11 weeks, more than 12 weeks, and 3-6 months." It was determined that four participant (50%) obtained 4-7 weeks of training, one participant (13%) trained 8-11 weeks, one participant (13%) trained more than 12 weeks, and two participants (25%) had 3-6 months of training (see Figure 2). It can be stated that eight of the eleven participants are involved with Unmanned Aircraft Systems operations within a law enforcement department. However, the other three participants may assist Unmanned Aircraft Systems operations within law enforcement departments but without acquiring training. Therefore, these results indicated that the majority of the participants, who answered this question, typically trained approximately 4-7 weeks for operating Unmanned Aircraft Systems.

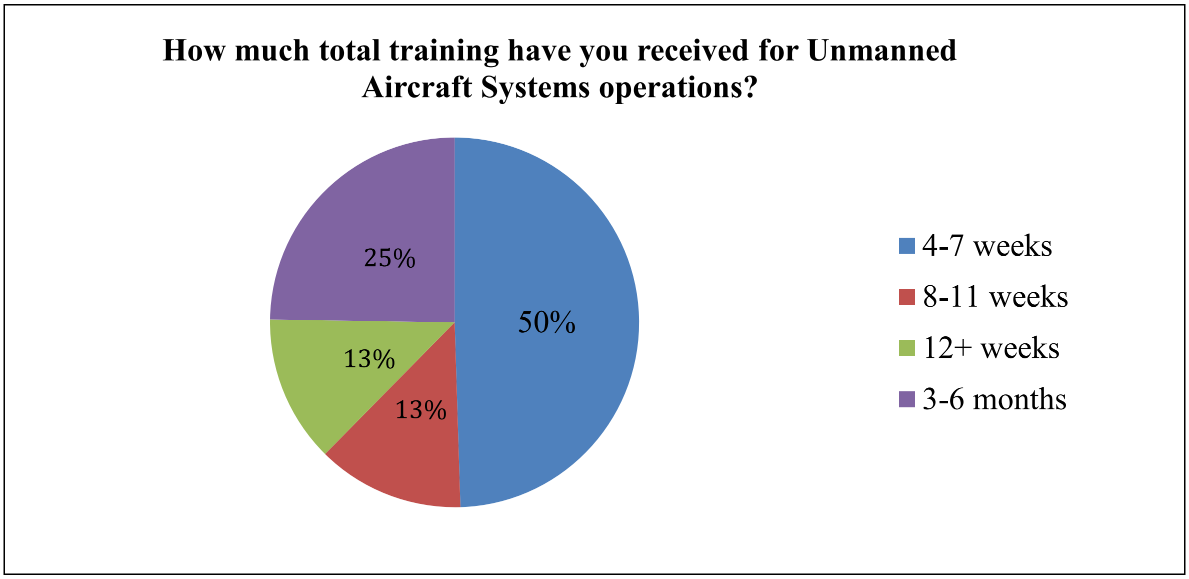


Figure 2. Total training in Unmanned Aircraft Systems operations

After distinguishing how much total unmanned aircraft systems training each participant received, it was also pertinent to ask, “How much total operational experience you received for Unmanned Aircraft Systems operations?” as asked in survey question six. Eight of the eleven participants answered question six, which included answer selections of “less than a month, 1-3 months, 4-7 months, 8-11 months, 1-2 years, more than 2 years, or other (please specify).” One participant (13%) answered that they acquired 1-3 months of total operational experience. Six participants (75%) obtained more than 2 years of total operational experience. However, one participant (13%) answered the “other” option and specified that they did not obtain operational experience.

Once again, it can be stated that seven of the eleven participants are involved with Unmanned Aircraft Systems operations within a law enforcement department (omitting one of the participants due to the statement of not obtaining operational experience for Unmanned Aircraft Systems). The other three participants may assist Unmanned Aircraft Systems operations within law enforcement departments but without acquiring

Unmanned Aircraft Systems operational experience. Therefore, these results indicated that the majority of the participants, who answered this question, obtained more than two years of total operational experience for Unmanned Aircraft Systems.

To continue with research on the cyber security vulnerabilities with law enforcement Unmanned Aircraft Systems, it was important to understand what type of FAA training certifications, if any, that participants possess. This allowed comparisons between the participants' answers to distinguish if their answers on cyber security concerns vary based upon their experience and FAA certifications. Therefore, "What level of FAA training do you possess?" was asked with choices of "private ground school, sport/recreational pilot certificate, private pilot certificate, above private pilot certificate (i.e. commercial, CFI), or no FAA flight training." It was determined that three participants (27%) obtained a private pilot certificate and three participants (27%) obtained a certificate above private pilot. However, five participants (45%) did not acquire any FAA flight training.

In order to determine if there were any cyber security vulnerabilities experienced by unmanned aircraft systems among law enforcement officers, "How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement Department or the Law Enforcement Department you assist with?" was asked. The responses included "very effective, effective, neutral, not very effective, and not at all effective." It was determined that three participants (27%) had answered very effective, four participants (36%) answered effective, two participants (18%) answered neutral, and two participants (18%) answered not very effective. For this question, it can be stated that 63% (27% very effective added to 36% effective) of participants believed that the Unmanned Aircraft Systems in the law enforcement they are involved or assisted with complete tasks at minimum, effectively (see Figure 3).

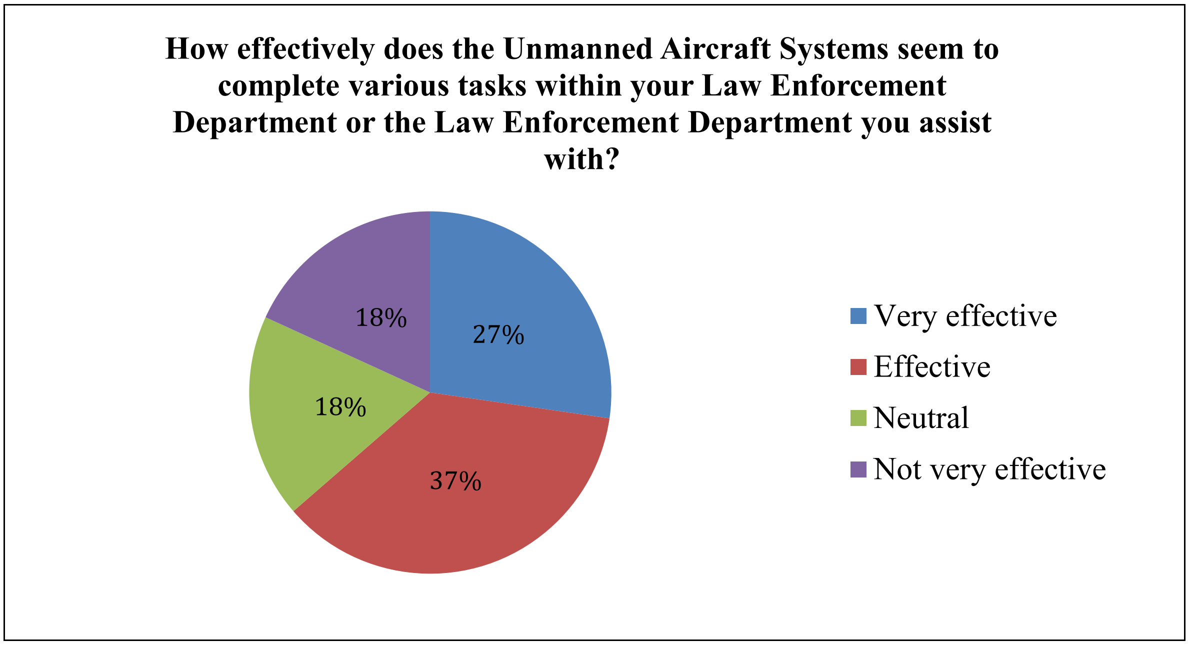


Figure 3. Effectiveness of UAS at completing tasks

The next question that was asked was, “Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?” Choices for this question comprised “very secure, secure, neutral, not very secure, and not at all secure.” It was recorded that one participant (9%) responded very secure, four participants (36%) replied secure, four participants (36%) answered neutral, and two participants (18%) responded not very secure regarding the security of the data link (control system) for unmanned aircraft systems (within their law enforcement department or the law enforcement department they assist with).

It can be stated that 45% (9% very secure added to 36% secure) of participants believed that the Unmanned Aircraft System's data link in the law enforcement they are involved or assisted are at minimum, secured. This can illustrate that these participants have no concerns in the security of the data link. However, 36% of the participants answered neutral. It can be questioned if this particular question presented confusion among the participants. It is unclear if the participants did not understand or know the answer to the question, if the participants did not think the data link is secured or not secured for law enforcement Unmanned Aircraft Systems, or if the participants are not involved or assisted with the Unmanned Aircraft Systems to the extent of being able to provide an answer.

The following question inquired, "Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist with are?" Choices for this question included "very secure, secure, neutral, not very secure, and not at all secure." One participant (9%) responded very secure, four participants (36%) replied secure, four participant (36%) answered neutral, and two participants (18%) responded not very secure regarding the security of the data link (control system) for unmanned aircraft systems (within their law enforcement department or the law enforcement department they assist with) (see Figure 4).

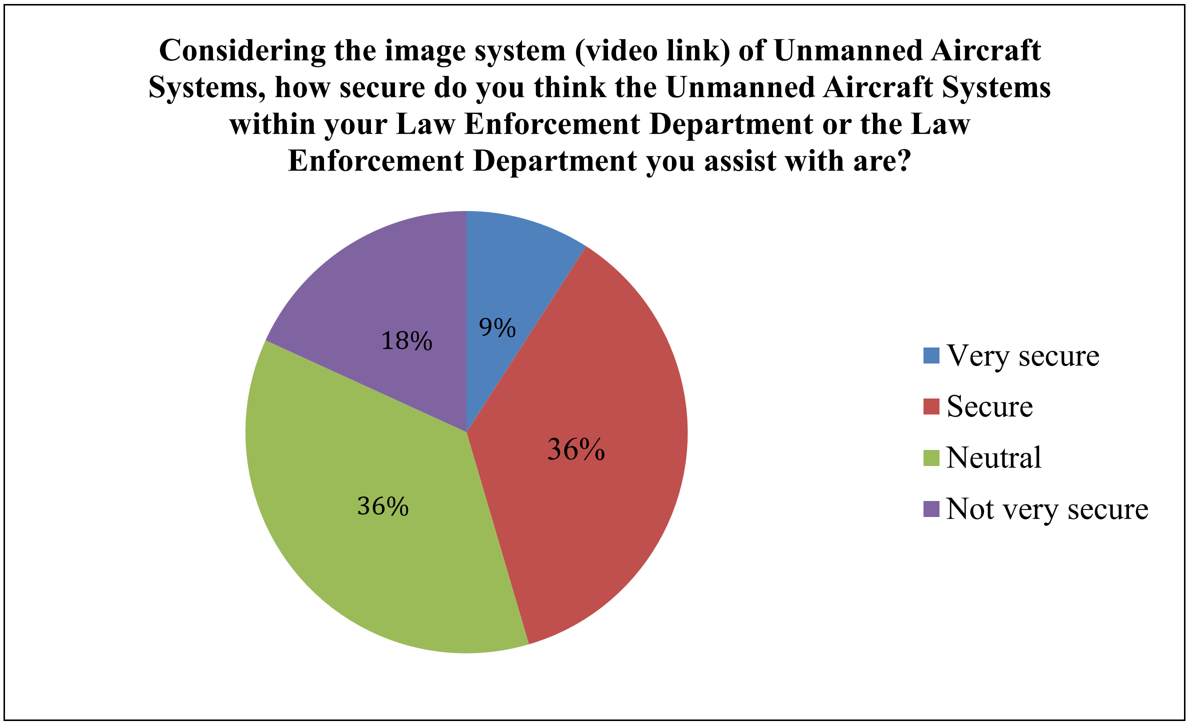


Figure 4. Security of video link of UAS

It can be stated that 45% (9% very secure added to 36% secure) of participants believed that the Unmanned Aircraft System's video link in the law enforcement they are involved or assisted are at minimum, secured. This can illustrate that these participants have no concerns in the security of the video link. However, 36% of the participants answered neutral. Again (and for further questions that obtain the "neutral" selection), it can be questioned if this particular question presented confusion among the participants.

To investigate further, the question, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during operational use?" was asked. The participants responded to the question by answering either "very likely, likely, neutral, not very likely, and not at all likely." One participant (9%) replied that they thought it was very likely for an Unmanned

Aircraft System to be hacked during operational use, while five participants (45%) responded that it was likely for unmanned aircraft systems to be hacked during operational use. However, one participant (9%) responded as neutral, but three participants (27%) answered not very likely and one participant (9%) stated that they believed it is not at all likely for unmanned aircraft systems to be hacked during operational uses (see Figure 5). This can signify that 54% of participants believe and have concerns that law enforcement Unmanned Aircraft Systems are at minimum, likely, to be hacked during operational uses.

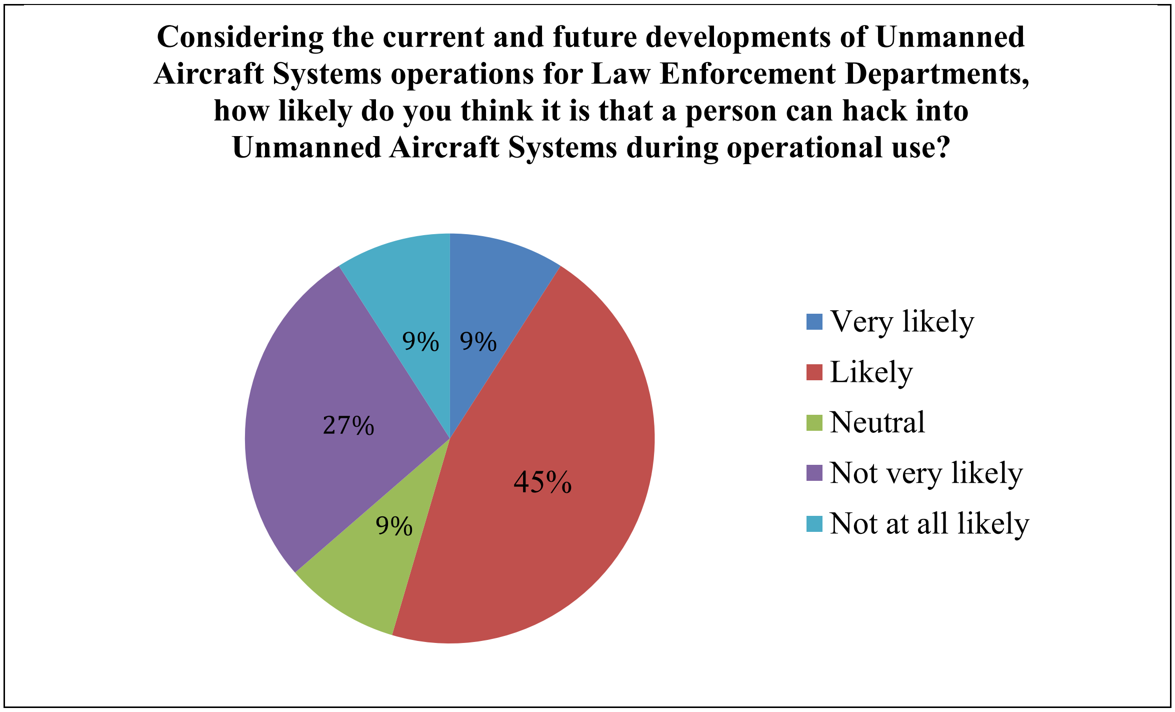


Figure 5. Possibility of hacking for Law Enforcement UAS

Since it was inquired if Unmanned Aircraft Systems would be hacked during operational uses, it was also useful to acquire information regarding if it was thought if the unmanned devices could be hacked during nonoperational uses in order to determine if different phases of Unmanned Aircraft Systems are more at risk for hacking. Therefore, “Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think a person can hack into Unmanned Aircraft Systems during nonoperational use?” was asked. The eleven participants responded to the question by answering either “very likely, likely, neutral, not very likely, and not at all likely.” Three participants (27%) replied that it was likely for an unmanned aircraft system to be hacked during nonoperational use, while five participants (45%) responded that it was not very likely and three participants (27%) replied that it was not at all likely for unmanned aircraft systems to be hacked during nonoperational use. This implies that 72% of participants believe and have no concerns that law enforcement Unmanned Aircraft Systems are, at minimum, not very likely to be hacked during nonoperational uses.

The next question that was asked was “How likely do you think it is for a person who hacks into an Unmanned Aircraft System to pose harm for public safety?” Selections for the answers included “Very likely, likely, neutral, not very likely, and not at all likely.” Data that was collected determined that two participants (18%) responded that it was very likely and three participants (27%) answered that it was likely for unmanned aircraft systems to be hacked that would pose harm on public safety, while two participants (18%) replied neutral. However, four participants (36%) responded that it was not very likely for a person to hack into an unmanned aircraft system to pose harm on public safety (see Figure 6).

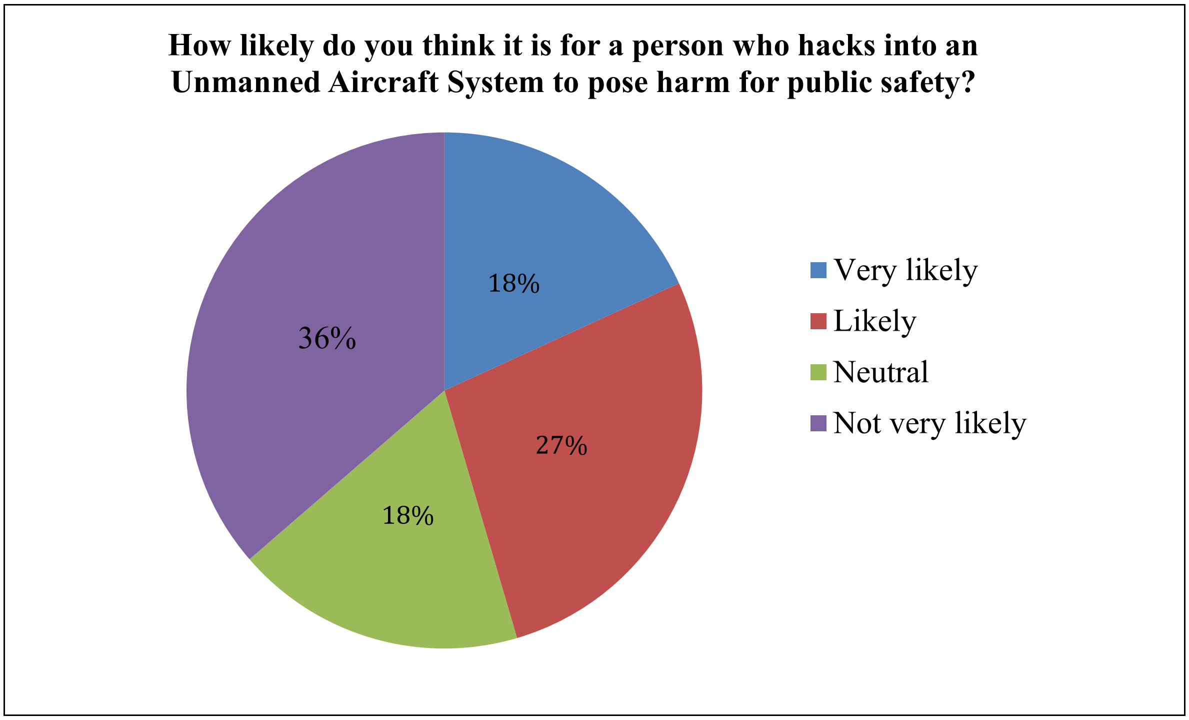


Figure 6. Effect of hacking of UAS on public safety

It is indicated that 45% of participants believe that law enforcement Unmanned Aircraft Systems are at minimum, likely, to be hacked for public safety harm. However, this percentage is lower compared the percentage of participants (54%) that stated it is a minimum, likely for a law enforcement Unmanned Aircraft Systems to be hacked. This differentiation in percentages may indicate that those who are involved or assisted with law enforcement departments that utilized Unmanned Aircraft Systems may believe the unmanned may be hacked, but hacked for other purposes other than for public harm. The above results are depicted in pie graphs below.

The last two questions that were asked are categorized as open-ended questions. This gave more of a personal perspective from the participants on their views about the cyber security vulnerabilities with law enforcement unmanned aircraft systems. Question 14 asked, "What are some security risk concerns you have for the use of Unmanned

Aircraft Systems for Law Enforcement Department that may affect public safety?" Six of the eleven participants responded to the open-ended question. The first participant's personal response included: "Inadequate trained personnel establishing LE UAS [law enforcement unmanned aircraft systems] units and operating UAS in an irresponsible manner." The second participant responded, "Hacking into the video feed would provide the person of interest with a view of what the public agency is capturing." The third participant replied that they did not have any concerns at this time while the fourth participant answered "Data security; control security." The fifth participant responded "malfunction" and the sixth participant replied that the "Video being seen by unauthorized personnel" could be detrimental.

Even though not all eleven participants answered this particular survey question and one participant who answered stated that they had no concerns at this time, a trend can be analyzed. Three of the six participants identified their security risk concern that the video data on Unmanned Aircraft Systems is vulnerable. However, in order to support that the trend is significant, more participation was needed for the study.

The last open-ended question asked, "What are some preventive cyber hacking measures your Department or Law Enforcement Department implements on Unmanned Aircraft Systems?" Seven participants responded. The first participant explained that "All systems are digital. Two of our four systems use digital encryption for both command and control and data links. All images are deleted from UAS and UAS laptops after 10 days. Retained images are stored on a secure server." The second participant briefly mentioned "Mil Spec navigation system" while the third participant replied that, "The OEM must implement a 128 bit encryption protocol so that this problem may be solved similar to military grade C2." The fourth participant responded, "We rely on the manufacturer to provide appropriate security." Lastly, the fifth participant briefly mentioned that their Department utilizes encryption and that the sixth participant responded as "N/A" [non-applicable].

Again, not all eleven participants, but seven participants answered this particular survey question. Each response was insightful and provided different techniques and procedures on preventive measures for cyber hacking. Even though two of the seven participants identified that they utilized encryption methods to secure Unmanned Aircraft Systems, it is not significant enough to determine a trend. Therefore, more participation is needed.

After analyzing each question as a whole (distinguishing the most common answer), each question was analyzed based on individual answers. This is to distinguish any trends that influenced specific answers regarding the years of experience with a law enforcement department, the amount of Unmanned Aircraft Systems operational experience, amount of Unmanned Aircraft Systems training, and level of FAA training.

The first survey question, "Approximately how long have you been working in Law Enforcement or assisting with Law Enforcement" was analyzed by comparing individual answers to search for commonalities or trends in specific answers. As mentioned previously, seven participants specified that they obtained at least 25 years of experience, one participant specified that they acquired between 21-24 years of experience, one participant answered that they had 16-20 years of experience, two participants selected obtaining 11-15 years of experience, and one participant answered having 6-10 years of experience with a law enforcement department (whether they were an officer or another personnel from another department that assisted with the law enforcement department). It is important to analyze the other survey question to compare commonalities among security concerns with law enforcement UAS.

For example, was there a common trend with survey question 3, “How often does your Law Enforcement Department or the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems?” This was to examine whether or not the amount of experience with a law enforcement department influences answers to each survey question. It is important to note that years of experience is referencing to the amount of experience that each participant obtained with a law enforcement department throughout this section unless specified otherwise. For this question, three participants with at least 25 years, one participant with 21-24 years, one participant with 16-20 years, and one participant with 11-15 years of experience with a law enforcement department specified that they were not sure on how often their Department utilizes UAS. However, one participant with at least 25 years and one participant with 11-15 years of experience replied that their Department utilizes UAS once per month. Two participants with at least 25 years and one participant with 6-10 years of experience replied that their Department utilized UAS twice a month**.**

Question 5, “How much total training have you received for Unmanned Aircraft Systems operations” was analyzed next. Eight of the eleven participants answered this question. Two participants with at least 25 years of experience acquired three to six months of total training for UAS operations, while one participant with at least 25 years of experience acquired 8-11 weeks of total training for UAS. Two participants with at least 25 years, one participant with 11-15 years of experience, and one participant with 6-

10 years of experience acquired four to seven weeks of total training for UAS operations. However, one participant with 11-15 years of experience acquired at least 12 weeks of total training for UAS operations.

Question 6, “How much total operational experience have you received for Unmanned Aircraft Systems operations?” was also important to examine. Unfortunately, only eight of the eleven participants answered this question. Four participants who acquired at least 25 years, and two participants who acquired 11-15 years of experience with a law enforcement department, obtained at least two years of total operational experience for UAS. However, one participant who acquired at least 25 years of experience selected the “other” choice and specified that they had no operational experience with UAS and one participant with 6-10 years of experience acquired one to three months of total operational experience.

Question 7, “What level of FAA training do you possess?” was also examined. Two participants with at least 25 years, one participant with 21-24 years, one participant with 16-20 years, and one participant with 11-15 years of experience obtained no FAA training. Two participants with at least 25 years and one participant with 11-15 years of experience acquired a private pilot certificate, while two participants with at least 25 years and one participant with 6-10 years of experience acquired above a private pilot certificate (i.e. Commercial, CFI).

Question 8, “How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement Department or the Law Enforcement Department you assist with?” was analyzed next. Six of the eleven participants who answered this question acquired at least 25 years of experience with a law enforcement department. Three of those six participants answered that UAS completed various tasks very effectively, while the remaining three replied that UAS completed various tasks effectively. One participant with 21-24 years and one participant with 16-20 years of experience answered neutral (neither agreeing or disagreeing) with the question. Two participants with 11-15 years of experience thought UAS completed various tasks not very effectively, while one participant with 6-10 years of experience believed that UAS completed various tasks effectively.

It is also important to distinguish any common trends with survey questions 9 and 10, “Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?” and “Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?” One participant with at least 25 years of experience answered very secure for both questions, while two participants answered not very secure and three participants answered secure for both questions. However, one participant of the 21-24 years, one participant of the 16-20 years, and two participants of 11-15 years of experience categories answered neutral for both questions 9 and 10. One participant from the 6-10 years of experience category answered secure for both questions.

The next question that was analyzed to determine any trends was question 11, “Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during operational use?" Of the participants who acquired at least 25 years of experience, one participant selected not at all likely, three participants thought it was not very likely, one participant believed it was very likely, and one participant selected neutral. However, one participant each from 21-24 years, 16-20 years, 6-10 years, and two participants from the 11-15 years of experience within a law enforcement department believed it was likely to hack into an UAS during operational use.

Another question that was analyzed was question 12, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during non-operational use?" Three participants who acquired at least 25 years of experience with a law enforcement department selected not at all likely for UAS to be hacked during non-operational use. However, three participants who also acquired at least 25 years of experience with law enforcement believed that it was not very likely for a person to hack an UAS during non-operational use. One participant with 21-24 years, one participant with 11-15 years, and one participant with 6-10 years of experience thought that it was likely to hack an UAS during non-operational use. One participant with 16-20 years and one participant with 11-15 years of experience believed that it was not very likely for a person to hack an UAS during non-operational use.

Question 13, "How likely do you think it is for a person who hacks into an Unmanned Aircraft Systems to pose harm for public safety" was also analyzed. Three participants with at least 25 years of experience with a law enforcement department believed that it was likely for a person to hack an UAS and pose harm on public safety;

however, three other participants who also acquired at least 25 years of experienced believed that it was not very likely to pose harm on public safety with a hacked UAS. One participant with 21-24 years of experience believed that it was not very likely, while one participant with 16-20 years and one participant with 11-15 years of experience believed it was very likely to pose harm with a hacked UAS. However, one participant with 11-15 years of experience and one participant with 6-10 years of experience answered neutral (neither agreeing or disagreeing) that hacked UAS poses harm for public safety.

Question 14, "What are some security risk concerns you have for the use of Unmanned Aircraft Systems for Law Enforcement Departments that may affect public safety?" was another question that was examined. This question was an open-ended question where participants typed their answers. Six of the eleven participants answered this question. Four of the six participants that answered this question acquired at least 25 years of experience with a law enforcement department. The answers that were recorded included that data and control security, inadequate training and utilizing UAS in an irresponsible manner, and hacking into the UAS video feed were security risks concerns that were believed to be an issue for these participants. It is also important to note that one of the four participants with at least 25 years of experience replied that they did not have any security risk concerns. Another participant with 16-20 years of experience replied that malfunction is a security risk, while a participant with 11-15 years of experience thought if unauthorized personnel views an UAS video feed could be a security risk concern.

After question 14 was analyzed, “What are some preventive cyber hacking measures your Department or Law Enforcement Department implements on Unmanned Aircraft Systems?” was examined. Again, this question was an open-ended question where participants could type in their own answers. Unfortunately, only seven of the eleven participants answered this question. Four of the seven participants who answered this question replied that encryption, military specialization navigation systems, and relying on the manufacturer for security are preventive measures that their Department utilizes against cyber hacking. However, one participant with 11-15 years of experience and one participant with 6-10 years of experienced answered that encryption was utilized as a preventive cyber hacking measure. It is also important to note that one participant, who acquired 16-20 years of experience replied “N/A” (non-applicable) as their answer.

After the first survey question was analyzed in more detail, survey question 7, “What level of FAA training do you possess?” was examined. This question was analyzed to determine any trends with answers from the other survey questions that were based on the participants’ level of FAA training. Otherwise, does a certain level of FAA training influence answers and by obtaining a higher level of FAA training, does it enhance more knowledge of security concerns with Unmanned Aircraft Systems.

Survey question 3, “How often does your Law Enforcement Department or the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems?” was compared with the level of FAA training. Five participants who did not acquire FAA training and one participant who obtained above a private pilot certificate was not sure how often UAS was utilized within the Department. Two participants with a private pilot certificate answered that their Department utilized UAS once a month, while one participant with a private pilot certificate and two participants with above private pilot certificate believed their Department utilized UAS twice a month.

Question 5, “How much total training have you received for Unmanned Aircraft Systems operations” was analyzed next. Eight of the eleven participants answered this question. One participant who did not acquire any FAA training and one participant who acquired above private pilot certificate specified that they obtained three to six months of total training for UAS operations. One participant who also did not obtain FAA training specified that they had at least 12 weeks of total training for UAS operations. However, two participants who acquired a private pilot certificate and two participants who acquired above private pilot certificate had four to seven weeks of total training for UAS operations and that one participant with a private pilot certificate acquired 8-11 weeks of total training for UAS operations.

Question 6, “How much total operational experience have you received for Unmanned Aircraft Systems operations?” was examined next. Unfortunately, only eight of the eleven participants answered this question. It is also important to note that one participant, who did not obtain FAA training, selected the “other” choice but specified that they do not obtain any UAS operational experience. One participant with no FAA training, three participants with a private pilot certificate, and two participants with above private pilot certificate acquired at least two years of total operational experience. However, one participant with above private pilot certificate acquired one to three months of total operational experience for UAS.

The next question that was examined was “How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement

Department or the Law Enforcement Department you assist with?" Again, five participants did not acquire FAA training. Of those five participants, one participant answered very effective, two participants answered that they were neutral (neither agreeing or disagreeing), one participant selected effective, and one participant believed tasks were not very effectively completed by UAS. One participant who acquired a private pilot certificate believed that tasks were not very effectively completed by UAS. However, two participants who obtained a private pilot certificate believed tasks were completed very effectively by UAS and that three participants believed that tasks were completed effectively by UAS.

Question 9, "Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?" was also examined. Of the participants who did not obtain FAA training, one participant believed that the data link was very secure, while three participants neither agreed nor disagreed on the security of the data link and one participant thought the data link of UAS was not very secure. However, one participant who acquired a private pilot certificate neither agreed nor disagreed, while two participants thought the data link was secured for UAS. One participant who obtained above a private pilot certificate believe that the data link was not very secure, while two participants with above private pilot certificate thought the data link was secured.

Question 10, "Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?" was also examined. Of the participants who did not obtain FAA training, one participant believed that the video link was very secure, while three participants neither agreed nor disagreed on the security of the video link and one participant thought the video link of UAS was not very secure. However, one participant who acquired a private pilot certificate neither agreed nor disagreed, while two participants thought the video link was secured for UAS. One participant who obtained above a private pilot certificate believed that the video link was not very secure, while two participants with above private pilot certificate thought the video link was secured.

Question 11, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during operational use?" was analyzed. The participants who did not have FAA training; one participant answered that it was not at all likely, three participants answered that it was likely, and one participant answered the it was very likely that UAS can be hacked during operational use. Those participants who acquired a private pilot certificate; one participant answered that it was likely, one participant answered that it was not very likely, and one participant neither agreed or disagreed (neutral) that UAS can be hacked during operational use. However, those participants who acquired above a private pilot certificate, two participants believed that it was not very likely and one participant believed that it was likely to hack into an UAS during operational use.

The following was asked question 12: "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft

Systems during non-operational use?” Of the participants who did not have FAA training: one participant answered that it was not at all likely, two participants believed that it was likely, and two participants thought that it was not very likely that UAS can be hacked during non-operational use. Those who obtained a private pilot certificate, one participant thought it was not very likely, while two participants believed it was not at all likely for UAS to be hacked during non-operational use. However, participants with above private pilot certificate, two participants answered that it was not very likely and one participant thought it was likely to hack an UAS during non-operational use.

The next question that was examined was, “How likely do you think it is for a person who hacks into an Unmanned Aircraft Systems to pose harm for public safety?” Of those participants who have no FAA training, one participant thought it was likely, two participants thought it was very likely, and two participants thought it was not very likely to pose public safety harm with a hacked UAS. Of those who acquired a private pilot certificate, one participant neither agreed nor disagreed, one participant thought it was not very likely, and one participant thought it was likely to pose harm on public safety with a hacked UAS. However, participants with above private pilot certificate, one participant thought it was likely, one participant neither agreed nor disagreed, and one participant thought it was not very likely to hack an UAS to pose harm on public safety.

Another question that was examined was, “What are some security risk concerns you have for the use of Unmanned Aircraft Systems for Law Enforcement Departments that may affect public safety?” It is important to note that six participants out of the eleven participants answered this and that one participant (who had acquired a private pilot certificate) replied that they did not have any security risk concerns. Two participants who did not obtain FAA training believed that malfunction and unauthorized personnel viewing UAS video feed as security risk concerns. One participant who had a private pilot certificate thought a security risk would be established if unauthorized personnel viewed video feeds. Two participants who obtained above a private pilot certificate thought that data and control security and inadequate training were security risk concerns for UAS.

Question 15, “What are some preventive cyber hacking measures your Department or Law Enforcement Department implements on Unmanned Aircraft Systems?” was analyzed. Seven of the eleven participants answered this question; however, one participant (who did not obtain FAA training) replied “not applicable”. Therefore, only participants with some FAA training answered this question. One participant with a private pilot certificate and three participants with above a private pilot certificate answered encryption were utilized as a preventive cyber security measure. However, two participants with a private pilot certificate, one participant answered that their Department relies on the manufacturer for security and the other participant’s Department utilizes military specialization navigation systems.

The next survey question that was analyzed in more thorough detail was, “How much total operational experience have you received for Unmanned Aircraft Systems operations?” It is important to note that three of the eleven participants had skipped answering this question; however, these participants had answered the other survey questions that will be discussed in this section (unless otherwise noted).

This question was analyzed by distinguishing any trends of common answers with other survey questions regarding security risks for Unmanned Aircraft Systems. The answers to question 3, “How often does your Law Enforcement Department or the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems**?”** was examined first. Three of the participants who had skipped the total operational experience question, two participants with at least two years of operational experience, and the participant who selected the “other” choice and specified they did not acquire any operational experience with Unmanned Aircraft Systems, answered that they were not sure of the Unmanned Aircraft Systems utilization frequency within the law enforcement department they were involved in. However, two participants with at least two years of operational experience replied that their law enforcement department utilized Unmanned Aircraft Systems once a month. There were two participants with at least two years of operational experience and one participant with one to three months of operational experience that thought their Department utilized Unmanned Aircraft Systems twice a month.

Question 5, “How much total training have you received for Unmanned Aircraft Systems operations?” was analyzed next. Three of the eleven participants, who skipped answering the initial question, also skipped this question. Three participants who acquired at least two years of total operational experience and one participant who acquired one to three months of total operational experience answered that they obtained four to seven weeks of total training for Unmanned Aircraft Operations. One participant who acquired at least two years of experience and one participant who selected the “other” option, but specified that they had no operational experience answered that they obtained three to six months of total training for Unmanned Aircraft Systems. One participant responded with at least two years of operational experience had achieved 8-11 weeks of training, while another participant with at least two years of operational experience achieved at least 12 weeks of total training for Unmanned Aircraft Systems.

The next question that was examined was “How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement Department or the Law Enforcement Department you assist with?” The three participants who skipped the initial question were divided as: one participant thought that tasks were completed very effectively by Unmanned Aircraft Systems, while two of the participants neither agreed nor disagreed on the effectiveness of task completion by Unmanned Aircraft Systems. Six participants with at least two years of operational experience was also divided as: two participants believed tasks were completed not very effectively, two participants thought tasks were completed effectively, and two participants thought tasks were completed very effectively. However, the participant who selected the “option” choice and the one participant who acquired one to three months of operational experience believed that Unmanned Aircraft Systems completed tasks effectively.

Question 9 and 10, “Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?” and “Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?” was examined next. Three of the participants who skipped the total operational experience question were recorded as: one participant believed that the data link was very secure and two participants neither agreed nor disagreed on the security of the data and video link. However, those with at least two years of operational experience was interpreted as: two participants neither agreed nor disagreed, one participant believed the links were not very secure, and three participants thought that the data and video links were secured. The participant who answered the "other" option believed that the links were not very secure, while the participant who acquired one to three months of operational experience thought the data and video link systems were secured.

The next analyzed question was, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during operational use?" One of the participants who skipped the initial question thought that it was not at all likely that a person could hack into an Unmanned Aircraft System during operational, while two of those participants believed it was likely. Six of the participants who obtained at least two years of operational experience, two of those participants believed it was likely, three of those participants thought it was not very likely, and one participant neither agreed nor disagreed with the potential of a person hacking into an Unmanned Aircraft System during operational use. The participant who answered the "other" option for the operational experience believed it was very likely, while the participant who obtained one to three months of operational experience believed that it was likely to hack into an Unmanned Aircraft System during operational use.

Question 12, "Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during non-operational use?"

was examined next. One of the participants who skipped the initial question thought that it was not at all likely that a person could hack into an Unmanned Aircraft System during non-operational use, one participant believed that it was not very likely, and one participant thought it was likely for a person to hack into an Unmanned Aircraft System during non-operational use. Six of the participants who obtained at least two years of operational experience, three participants believed it was not very likely, two participants believed it was not at all likely, and one participant believed it was likely for Unmanned Aircraft Systems to be hacked during non-operational use. The participant who answered the “other” choice for the operational experience thought it was not very likely, while the participant who obtained one to three months of operational experience believed that it was likely for a person to hack into an Unmanned Aircraft System during non-operational use.

Question 13, “How likely do you think it is for a person who hacks into an Unmanned Aircraft Systems to pose harm for public safety?” was also examined. The three participant who skipped the operational experience question was divided into, one participant believed it was likely, one participant thought it was very likely, and one participant believed it was not very likely for a hacked Unmanned Aircraft System to pose harm on public safety. Six participants with at least two years of operational experience was also divided similarly: one participant neither agreed nor disagreed, two participants believed it was likely, one participant believed it was very likely, and two participants thought it was not very likely for a hacked Unmanned Aircraft System to pose harm on public safety. However, the participant who answered the “other” option believed it was not very likely, but the participant with one to three months of operational experience neither agreed nor disagreed with a hacked Unmanned Aircraft System posing harm on public safety.

The next question, “What are some security risk concerns you have for the use of Unmanned Aircraft Systems for Law Enforcement Departments that may affect public safety?” was also examined. As noted previously, this was an open-ended question where participants typed in their own answers. However, six of the eleven participants answered this question and one of those participants had replied that they did not have any security risk concerns at this time. One of the six participants had skipped the operational experience question but answered that they believed malfunction was a security risk concern for Unmanned Aircraft Systems. Those participants with at least two years of experience believed that inadequate training, data and control security, and video being seen by unauthorized personnel were security risk concerns for Unmanned Aircraft Systems. However, the participant who answered the “other” option also believed that the accessing video feed from unauthorized personnel was a security risk concern.

Question 15, “What are some preventive cyber hacking measures your Department or Law Enforcement Department implements on Unmanned Aircraft Systems?” was another open-ended question that was analyzed. Seven of the eleven participants answered this question; however, one of those seven participants replied “N/A” (non-applicable). Those with at least two years of experience were divided into: three participants believed encryption, on participant thought relying on the manufacturer, and one participant believed military specialization navigation systems were preventive cyber hacking measures.

Literature Analysis

In the research study's survey, it is indicated that there is a concern that law enforcement unmanned aircraft systems can be hacked. Therefore, this assumption warrants additional research through a literature analysis. It is important to acknowledge what resources hackers have that would allow them to successfully collect confidential data from Law Enforcement Unmanned Aircraft Systems. As previously mentioned in chapter two of this study, specific resources were gathered from searching the Google database, along with MTSU Library's JEWL search engine and the Academic Search Premier database for relevant topics on cyber security on Unmanned Aircraft Systems. Keywords that were utilized within the search included: cyber security, UAS, unmanned aircraft systems, resources for hackers, cyber security and unmanned aircraft systems, hacking, hacking UAS, law enforcement unmanned aircraft systems, components of UAS, and systems of UAS. Resources were selected based on those criteria, which successfully answered research question number one. Again, there were other resources that were discovered but were not utilized for the study because of repetitive information, lack of information, or the information was irrelevant to the topic.

Cyber security hacks can be classified into three groups: sensor spoofing, wireless attacks, and hardware attacks. Sensor spoofing occurs when falsified data is transmitted through the Unmanned Aircraft Systems autopilot's on-board sensors. These sensors include lidar, IR sensors, radar, sonar, vision, and GPS receivers. Attackers may transmit falsified data through GPS channels or blinding the vision sensors. This is critical and is expressed of importance to protect because Unmanned Aircraft Systems autopilots rely on the sensor data for Guidance and Navigation (Kim et al., 2011).

Wireless attacks occur if the attacker hacks into the encrypted communication channel. If the attacker succeeds in this hack then the attacker will be able to alter the on-board data of the autopilot through the wireless communication channel. After this occurs, full control of the Unmanned Aircraft Systems is achieved. Another attack is possible through a buffer overflow. This initiates some event or corrupts the data on-board. Wireless attacks can be achieved from afar by the attacker (Kim et al., 2011).

Hardware attacks is another classification of cyber hacking. This transpires when the attacker achieves direct access to any component of the autopilot. The hacker can corrupt stored data on the autopilot or install other components that corrupt data flow. Hackers can complete this type of an attack during manufacturing, maintenance, storage, or delivery. Attackers have direct link to the autopilot and reprogram or damage the Unmanned Aircraft System, which then results in full control gained and collection of tactical data. This is essential to acknowledge because during this attack, data and control are compromised along with affecting the Unmanned Aircraft System survivability (Kim et al., 2011).

After acknowledging the different categorizes of cyber hacking, it is vital to understand the various technologies that are available to hackers to execute such attacks. For example, there is the SkyGrabber software, which is available “off the shelf.” Originally, the product was utilized to intercept satellite feeds of videos, television, and music. However, it was unknown to the owner of SkyGrabber that this software can be utilized to capture Unmanned Aircraft Systems feeds (Rivera et al., n.d.).

Another resource that is available is SkyJack. This software was released by Sammy Kamkar, an independent security analyst, and was utilized to take control of

Unmanned Aircraft Systems by another Unmanned Aircraft System through only a Wi-Fi network. This is achieved by the code transmitting from the ground linux machine or from another Unmanned Aircraft System within the same range as the targeted Unmanned Aircraft System. Once the Unmanned Aircraft System is recognized, it disconnects it from the ground station, and overrides its signal; thus, gaining full access of the targeted drone. In December 2013, Sammy Kamkar utilized the tiny Raspberry Pi computer, two wireless transmitters, and a battery and equipped those components on a Parrot AR Drone 2.0 in order to perform the hacking. He was able to take control of another Parrot Unmanned Aircraft System by utilizing the components equipped on the Parrot AR Drone 2.0 (Moskvitch, 2014; Rivera et al., n.d.).

Snoopy is another device that can be utilized. This software is used to take advantage of various electronic devices that utilize Wi-Fi networks by profiling and tracking such devices by an Unmanned Aircraft Systems as it imitates a recognized network. Snoopy software can also access Bluetooth, 802.15, and Radio Frequency Identification (RFID). This software can also obtain a person’s location along with their personal information along with data from cellular devices and requests and data transmitted over that particular network. However, even though this software has a negative connotation, it may be advantageous to emergency responders. For example, after an emergency situation (i.e. earthquake or tornado), this device may be utilized to search for survivors and tracking any movements of the survivors from their cellphones or other electronic devices. If responders are able to gain access to this information, it will prove beneficial in order to plan and search for areas of survivors (Rivera et al., n.d.).

As mentioned previously, one of the United States' military Unmanned Aircraft Systems, the RQ-170, was captured by the Iranian Government via spoofing. This was accomplished by jammed communications links of the Unmanned Aircraft System. The ground controllers were disconnected from the unmanned device and caused the unmanned aircraft to alter to autopilot. The Unmanned Aircraft System was forced to discover GPS frequencies that were unencrypted. Since the Iranian Government transmitted incorrect GPS coordinates, it caused the unmanned device to believe it was in its designated location and landed in Iran (Moskvitch, 2014).

During the literature analysis, a relevant research study was examined. Kerns, Shepard, Bhatti, & Humphreys' (2014) conducted a capture and control of an Unmanned Aircraft System by GPS spoofing. The researchers accessed Unmanned Aircraft Systems vulnerabilities through GPS signals by determining capture requirements and the range for the capture and demonstrated a field test to capture an Unmanned Aircraft System via GPS spoofing.

During the field demonstration, an unmanned aircraft hovered 8.8 m above ground, where the spoofer transmitted GPS signals to the unmanned device and the spoofer was able to capture the GPS receiver from the Unmanned Aircraft System. The device's velocity and position was accessed and controlled and sent the unmanned aircraft into a northward position. It was noted in the study that the spoofing attack went undetected due to a lack of checking against spoofing design feature on the Unmanned Aircraft System (Kerns, Shepard, Bhatti, & Humphreys, 2014).

Attacks can be established through signal jamming, signal blockage, and transmitting counterfeit signals to the Unmanned Aircraft System to operate the device's time, position, and velocity. These attacks can be achieved by purchasing equipment that are utilized against GPS receivers and that civilian Unmanned Aircraft Systems are unauthenticated and unencrypted, which are specified in public documents (Kerns et al., 2014).

Another relevant research study was also revealed during the literature analysis. A professor and five computer security graduate student team members from Johns Hopkins University uncovered three methods to interfere with Unmanned Aircraft Systems from a laptop. The students who were involved with this study were fulfilling a capstone project requirement. Their study was to establish Unmanned Aircraft Systems and wireless network penetration by exploits in order to expose vulnerabilities of the unmanned device (Sneiderman, 2016). Exploits are "a piece of software typically directed at a computer program or device to take advantage of a programming error or flaw in that device" (Sneiderman, 2016, para. 9). Therefore, the students sent approximately 1,000 wireless connection requests within rapid sequence, demanding control of the unmanned device. This sequence overloaded the Unmanned Aircraft System's processing unit, which shut down the device and caused it to land uncontrollably (Sneiderman, 2016).

The students also performed another hack with the Unmanned Aircraft System. The students transmitted a large data packet to the unmanned device (Sneiderman, 2016). This "exceeded the capacity of the buffer allocated for such information within the aircraft's flight application" and caused the Unmanned Aircraft System to crash (Sneiderman, 2016, para. 11). The students conducted the third exploit, which was sending a falsified digital packet to the Unmanned Aircraft System's controller from a laptop. This information transmitted falsified information by revealing that the unmanned device was transmitting the packet. This resulted in an emergency landing of the Unmanned Aircraft System (Sneiderman, 2016).

The literature analysis that was conducted revealed that hackers do have available resources in order to hack and collect confidential data from Law Enforcement Unmanned Aircraft Systems. Attacks can be executed through sensor spoofing, wireless attacks, and hardware attacks. Technologies are also available to accomplish hacking such as the SkyGrabber software, SkyJack software, and Snoopy software. It is essential to acknowledge such available resources in order to develop and implement recommendations and solutions to prevent such attacks. More information regarding recommendations and solutions for cyber hacking will be discussed in chapter four of this study.

It is also important to note that this chapter reported and reviewed answers that were collected from a survey in order to reveal a risk concern among unmanned aircraft systems. The data that was collected gathered background information about the participants, established trends and revealed possible limitations within the study, which will be explained more thoroughly in the following chapter.

CHAPTER IV DISCUSSION

The goal of this study was to determine cyber security vulnerabilities with Law Enforcement Unmanned Aircraft Systems. As part of seeking answers to this study, a survey was distributed and a literature analysis was conducted. Respondents to the survey included law enforcement departments and personnel who assist law enforcement departments that utilize UAS or have considered utilizing UAS. Respondents' feedback along with the literature analysis was collected and reviewed to answer the three research questions stated in Chapter One.

Research Question 1

The first research question was, "Based on literature analysis, what resources do hackers have that would allow them to successfully collect confidential data from Law Enforcement Unmanned Aircraft Systems?" To answer this question, a literature analysis was conducted and it was determined that yes, there are resources available for hackers to successfully collect confidential data from Unmanned Aircraft Systems. Hackers can accomplish cyber attacks such as sensor spoofing, wireless attacks, and hardware attacks. To execute such attacks, various technologies like the SkyGrabber software, SkyJack software, and Snoppy software can be accessed. Some of these technologies are readily available for customers to purchase "off the shelf."

Research Question 2

The second research question, "Do Law Enforcement Officers believe hackers can collect data from Law Enforcement Unmanned Aircraft Systems to pose harm on public safety, and what are those public safety concerns?" was also answered. Public safety is the protection and prevention against dangers such as disasters and crimes

(USLegal, 2016). In this study, it was pertinent to analyze public safety concerns regarding Law Enforcement Unmanned Aircraft Systems.

Data collection and analysis revealed that 63% of participants believed that unmanned aircraft systems completed various tasks at a minimum, effectively. It was also revealed that 45% of participants believed, at minimum, that the control system (data link) and the image system (video link) are secured. However, 54% of participants believed, at minimum, that it was likely possible to hack an unmanned aircraft system during operational use. However, 72% of participants believed that it was not very likely that the device would be hacked during non-operational use. It was also revealed that 45% of participants believed that it was likely a hacked unmanned aircraft system could pose harm for public safety.

Thus, the over arching answer to research question 2 is that the majority of Law Enforcement Officers do not believe hackers can collect data from Law Enforcement Unmanned Aircraft Systems to pose harm on public safety. But it was established that there was no clear opinion stated. In the collected data, it was recorded that 9% of the participants believed the systems (data and video links) were very secure and 36% of participants believed they were secure. However, 36% of participants answered “neutral” (neither agreeing or disagreeing about the security of those systems), while 18% of participants believed that the systems were not very secure. The conclusions that was drawn from the survey was that 45% of participants believed that the data and video links are secured; however, it was revealed that officers do have some concern about the device becoming hacked and utilized to pose harm. In order to better distinguish these concerns, additional research is warranted.

Research Question 3

The last research question answered was, “Do Law Enforcement officials view cyber hacking on Law Enforcement Unmanned Aircraft Systems as a security risk, and what are these security risk concerns?” The answer to this research question is yes, Law Enforcement officials do view cyber hacking on Law Enforcement Unmanned Aircraft Systems as a security risk. Security risk is the security of something that is potentially threatened by a situation or person (Random House Dictionary, 2016). As previously mentioned, it was revealed that 45% of participants believed, at minimum, that it was likely possible to hack these unmanned devices to pose harm for public safety. It was also revealed that these security risks include inadequate training for personnel, irresponsible operations, unauthorized access to such devices, hacking into the video feed, data and control security, and malfunction. However, some participants revealed preventive measures for cyber hacking. These preventive measures include encryption, relying on security from the manufacturer of the unmanned device, and deleting necessary files and retaining files on a secured server.

Recommendations

Considering that the study revealed available resources for hackers to successfully collect confidential data from UAS and Law Enforcement Officers and those who assist Law Enforcement Officers have UAS security risk concerns, it is essential to acknowledge and address all cyber security risks and vulnerabilities associated with Unmanned Aircraft Systems. Therefore it is required to implement countermeasures for risks and vulnerabilities. For example, corrective implementations in the GPS receivers’ software should be applied: amplitude discrimination and time-of-arrival discrimination.

This can also include techniques such as angle-of-arrival discrimination, consistency of navigation inertial measurement (IMU) crosscheck, cryptographic authentication, and polarization discrimination. Preventing attacks from GPS spoofing comprises the utilization of the cryptographic authentication while the transmitter and receiver utilizes a mutual authentication method to avoid any external source interferences. However, this type of method has only been developed and implemented for military Unmanned Aircraft Systems. Therefore, it is recommended that such processes are developed and implemented for civilian Unmanned Aircraft Systems (Paganini, 2013).

It is pertinent to study topics regarding Unmanned Aircraft Systems and safety and security issues. More specifically, researching cyber security vulnerabilities and law enforcement Unmanned Aircraft Systems. If unmanned vehicles are hacked, it could lead potential catastrophic events such as mid-air collision with manned aircraft and other significant impacts on the ground (i.e. people, vehicles, buildings, and other structures). These impacts can cause serious and fatal injuries along with severe damage. Therefore, it is vital that the various systems and components of Unmanned Aircraft Systems are improved with a back-up system that has the ability to recover from Unmanned Aircraft Systems during a hack (Carr, n.d.).

Previously, there has been approximately a billion dollar investment into a study for ground control stations and data links for Unmanned Aircraft Systems operations. The study indicated that frequency jamming and time delay (or latency) directly affects Unmanned Aircraft Systems operations accuracy. It is crucial that research continues for a “fail-safe system” to be successfully implemented. Previously, Todd Humphreys and his University of Texas at Austin team conducted research that allowed them to hack a

Department of Homeland Security Unmanned Aircraft System by utilizing equipment that cost approximately $1,000. Todd Humphrey and his team utilized the equipment to hack into the unmanned device's GPS signal that was only lightly encrypted. Therefore, his team and him expressed how vital it is to ensure that all Unmanned Aircraft Systems that are over 18 pounds acquire anti-spoofing technology (Carr, n.d.).

The data link and ground control stations infrastructure's security is a significant procedure in safe operations of Unmanned Aircraft Systems. These devices can present danger for the public because if those who desire terrorist harm capture the unmanned devices, then the Unmanned Aircraft Systems could become controlled for surveillance purposes, utilized as weapons, and other unlawful purposes. Components for Unmanned Aircraft Systems must be developed "spoof-proof" in order for the device to detect GPS data that had been compromised. For example, unsecured GPS for civilian Unmanned Aircraft Systems purposes will need a mechanism that will detect additional radio signals that are being received from the GPS hacker (spoofer) and in return would ignore any false data that is transmitted. It would also be highly beneficial for the Wide Area Augmentation System GPS to be encrypted; therefore, allowing additional multiple frequencies so that the Unmanned Aircraft System would receive multiple GPS bands, encrypting digital signatures into cross referencing or the GPS data, increasing the original GPS system (Carr, n.d.).

The vulnerabilities among Unmanned Aircraft Systems GPS exist and present risks for the public and the Unmanned Aircraft Systems operators. It is essential to ensure there is no interference within the Unmanned Aircraft Systems' GPS; therefore, the common data link (CDL) that connects the operator and the remote operating ground station must be secured. Unmanned Aircraft Systems entails two different radio communication links in order to operate. The first link supplies the Full Motion Video (FMV) to the Remote Viewing Terminal (RVT) through the Video Data Link (VDL) (utilizes omni-directional antenna). The second link allows the controlling of the Unmanned Aircraft Systems though the CDL, which allow the RVT that is synced with the VDL to examine the unmanned device's FMV. Depending on the signal strength of the VDL determines the video consistency and quality and that targeted jamming can result in the interference of the CDL and VDL. However, three potential electronic protections exist against such vulnerabilities: counter jammers, spectrum management, and electromagnetic (EM) hardening (Carr, n.d.).

Limitations

Unfortunately, the study presented limitations that need to be resolved in order to revisit and continue with future research of this topic. Originally, only law enforcement departments that utilize Unmanned Aircraft Systems were supposed to be contacted for voluntarily participation of the study. However, very few departments that utilize Unmanned Aircraft Systems exist due to the restraints of Unmanned Aircraft Systems regulations. Therefore, fewer departments were eligible for the study than anticipated. This can be resolved by altering the research to include different groups in the study (i.e. Unmanned Aircraft Systems organizations, Federal Aviation Administration, Law Enforcement Departments, et al) to acquire their input on cyber security vulnerabilities with law enforcement Unmanned Aircraft Systems. Another approach to this study may involve waiting for Unmanned Aircraft Systems regulations to be established, so that more law enforcement departments may be able to acquire Unmanned Aircraft Systems utilization.

Other limitation issues developed during the IRB approval process. Once confirmation was received that participants agreed to the research study, the IRB form was completed and sent to the College of Graduate Studies at MTSU. However, the form was returned because other documentation was needed to show proof that the participants agreed to partake in the survey. This delayed the approval process and caused the survey to be administered later than anticipated. Once the IRB approval was granted, the survey was administered. However, considering the delay, participants' schedule, and other factors, there was lack of survey participation from the participants from what had been expected based on initial e-mail contact.

Another problematic issue occurred when only 11 of the potential 16 participants completed the study. This caused a hindrance in the data analysis because there was not enough participants to thoroughly collect, analyze, and develop cyber security vulnerability trends. In order to acquire more accurate data, more participants must be gathered. This may be completed through contacting participants for survey interviews via phone or in person rather than e-mail correspondence.

Another limitation that existed was the lack of responses on the open-ended questions regarding cyber security risk concerns and preventive cyber hacking measures. Lack of participation with these questions could have resulted from participants not wanting to type in answers (just selecting a multiple-type answer question may have been more convenient). Another reason this could have resulted, especially with the preventive cyber hacking measures question, is that the participants' answers were confidential;

therefore, they could not respond. This could be potentially resolved by adding the question “Does your Law Enforcement Department or the Law Enforcement Department you assisted with have preventive cyber hacking measures for Unmanned Aircraft Systems?” This could at least distinguish if Departments do have preventive cyber hacking measures but may reveal that such measures are confidential and cannot be exposed.

Other limitations included that at the time of the research, there were minimum regulations developed and implemented. However, after the time this study was conducted, regulations were developed and implemented as described in Title 14 CFR Part 107. These regulations include detailed information regarding the operations (i.e. registration, medical conditions, hazard operations, and restrictions) and certifications for small unmanned aircraft systems. It is important to revisit this study and to examine and include Title 14 CFR Part 107 for future research.

Another limitation that existed was with the answer choices in some of the questions. Some of the answers may have been misleading or did not have the appropriate answer selection. For example, participants may have not been able to respond to a particular question because their answer was not a choice. This can be resolved by analyzing the question more thoroughly and adding more choices or adding, “other” to the answer choices and have the option for the participant to type in their own answer.

The final limitation experienced was the time constraint to conduct the research. For future research, more time to gather participants, administer the survey, and collect data should be considered. Additional time would be beneficial because it would allow for more accurate data to be established. This may be achieved by evaluating and obtaining the appropriate time length to successfully complete the study.

Future Research

In order to acquire a thorough understanding about cyber security vulnerabilities with law enforcement Unmanned Aircraft Systems, additional research should be considered. According to Rivera, Baykov, & Gu (n.d.), video receivers should be examined to determine whether or not encryption exists for Unmanned Aircraft Systems and also determine if the receivers could be compatible or be built to compatibility for Unmanned Aircraft Systems. Encryption is vital for Unmanned Aircraft Systems in order to protect video feeds from being accessed from unauthorized personnel. Along with the encryption determination, research should include discovering software that will check abnormalities within the Unmanned Aircraft Systems. This will allow the components to be protected from attacks. However, it is important to consider that such technological updates for Unmanned Aircraft Systems will be costly (Rivera et al., n.d.).

Another important study to include is researching on how operators respond to Unmanned Aircraft Systems and procedures to appropriately respond to such an attack. Other research should include examining cyber security vulnerabilities among specific types of Unmanned Aircraft Systems or different Unmanned Aircraft Systems manufacturers. This will allow comparison of any vulnerability that may exist on one type of Unmanned Aircraft System than another type. Cyber security vulnerabilities along with preventive measurers could be thoroughly examined and compared with military and civilian Unmanned Aircraft Systems.

REFERENCES

AUVSI. (n.d.). The benefits of unmanned aircraft systems: Saving time, saving money, saving lives. *Association for Unmanned Vehicle Systems International.* Retrieved from https://epic.org/events/UAS-Uses-Saving-Time-Saving-Money-Saving-Lives.pdf

Bunker, R. (2015). Conference report: Connecting the dots in unmanned aerial systems and cyber security. *Red Team Journal.* Retrieved from http://redteamjournal.com/2015/01/connecting-the-dots-conference/

Canis, B. (2015). Unmanned aircraft systems (UAS): Commercial outlook for a new industry. *Congressional Research Service.* Retrieved from https://fas.org/sgp/crs/misc/R44192.pdf

Carr, E. (n.d.). Unmanned aerial vehicles: Examining the safety, security, privacy, and regulating issues of integration into U.S. airspace. *NCPA.* Retrieved from http://www.ncpa.org/pdfs/sp-Drones-long-paper.pdf

Connor, R. (2015). This drone can save your life. *Air & Space Smithsonian,* 20-21.

Dunn, J. (2014). Drones show high promise for assisting law enforcement. *The North Bay Business Journal.* Retrieved from http://www.northbaybusinessjournal.com/csp/mediapool/sites/NBBJ/IndustryNews/story.csp?cid=4185811&sid=778&fid=181

FAA. (2015a). Federal Aviation Administration. *Unmanned Aircraft Systems: Public Operations (Governmental).* Retrieved from http://www.faa.gov/uas

FAA. (2015b). Federal Aviation Administration. *Unmanned Aircraft Systems: Civil Operations (Non-Governmental).* Retrieved from http://www.faa.gov/uas

FAA. (2015c). Federal Aviation Administration. *Unmanned Aircraft Systems: Model Aircraft Operations.* Retrieved from http://www.faa.gov/uas

FAA. (2016). Unmanned aircraft systems. *Federal Aviation Administration.* Retrieved from https://www.faa.gov/uas/

Greene, S. (2013). Mesa County, Colo. A national leader in domestic drone use. *The Huffington Post.* Retrieved from http://www.huffingtonpost.com/2013/06/06/mesa-county-colo-a-nation_n_3399876.html

Gupta, S., Ghonge, M., & Jawandhiya, P. (2013). Review of unmanned aircraft system (UAS). *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2*(4).

HSE. (2015). Homeland surveillance electronics. *Police UAV Drones: Remote Aerial Platform Tactical Reconnaissance Police UAV Drones.* Retrieved from http://www.policeuavdrones.com

IAFC. (2014). International Association of Fire Chiefs. *IAFC Position: Use of Unmanned Aerial Vehicles in Public Safety Emergency Response.* Retrieved from http://www.iafc.org/IAFC-position-Use-of-Unmanned-Aerial-Vehicles-In-Emergency-Response

Julian, T. (2014). Defining moments in the history of cyber-security and the rise of incident response. *Infosecurity Magazine.* Retrieved from http://www.infosecurity-magazine.com/opinions/the-history-of-cybersecurity/

Keane, J. & Carr, S. (2013). A brief history of early unmanned aircraft. *John Hopkins*

APL Technical Digest, 32(3). Retrieved from http://www.jhuapl.edu/techdigest/TD/td3203/32_03-Keane.pdf

Kerns, A. Shepard, D., Bhatti, J., & Humphreys, T. (2014). Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics, 31,* 617-636. doi : 10.1002/rob.21513

Kim, A., Wampler, B., Goppert, J., Hwang, I., & Aldridge, H. (2011). Cyber attack vulnerabilities analysis for unmanned aerial vehicles. *American Institute of Aeronautics and Astronautics.*

Mendez, C. (2014). Professor discusses the hacking of drones. *The Daily Texan.* Retrieved from http://www.dailytexanonline.com/2014/11/23/professor-discusses-the-hacking-of-drones

Moskvitch, K. (2014). Are drones the next target for hackers? *BBC News.* Retrieved from http://www.bbc.com/future/story/20140206-can-drones-be-hacked

NATO. (n.d.). The history of cyber attacks – a timeline. *NATO Review Magazine.* Retrieved from http://www.nato.int/docu/review/2013/cyber/timeline/EN/index.htm

Paganini, P. (2013). Hacking Drones…Overview of the Main Threats. *Infosec Institute.* Retrieved from http://resources.infosecinstitute.com/hacking-drones-overview-of-the-main-threats/

Paganini, P. (2012). Security affairs. *GPS Spoofing, old threat and new problems.* Retrieved from http://securityaffairs.co/wordpress/2845/hacking/gps-spoofing-old-threat-and-new-problems.html

Press. (2014). Emergency: Earthquake disaster response team uses flying cameras to aid relief efforts. *sUAS News.* Retrieved from http://www.suasnews.com/category/emergency/

Press, G. (2015). This week in tech history: The birth of the cybersecurity and computer industries. *Forbes.* Retrieved from http://www.forbes.com/sites/gilpress/2015/11/01/this-week-in-tech-history-the-birth-of-the-cybersecurity-and-computer-industries/#1dac955b6e4f

Random House Dictionary. (2016). Security risk. *Random House Dictionary.* Retrieved from http://www.dictionary.com/browse/security-risk

Rivera, E., Baykov, R., & Gu, G. (n.d.). A study on unmanned vehicles and cyber security.

Rodday, N. (2015). Exploring security vulnerabilities of unmanned aerial vehicles. *University of Twente.*

Sifton, J. (2012). The Nation: Instigating progress daily. *A Brief History of Drones: With the invention of drones, we crossed into a new frontier: killing that's risk-free, remote, and detached from human cues.* Retrieved from http://www.thenation.com/article/brief-history-drones/

Schwartz, M. (2012). GPS spoofer hacks civilian drone navigation system. *Information Week.* Retrieved from http://www.darkreading.com/vulnerabilities-and-threats/gps-spoofer-hacks-civilian-drone-navigation-system/d/d-id/1105117

Sneiderman, P. (2016). Johns Hopkins scientists show how easy it is to hack a drone and crash it. *Johns Hopkins University.* Retrieved from http://hub.jhu.edu/2016/06/08/hacking-drones-security-flaws/

Tomiuc, E. (2012). Features: Drones-Who makes them and who has them? *Radio Free*

Europe Radio Liberty. Retrieved from http://www.rferl.org/content/drones_who_makes_them_and_who_has_them/24469168.html

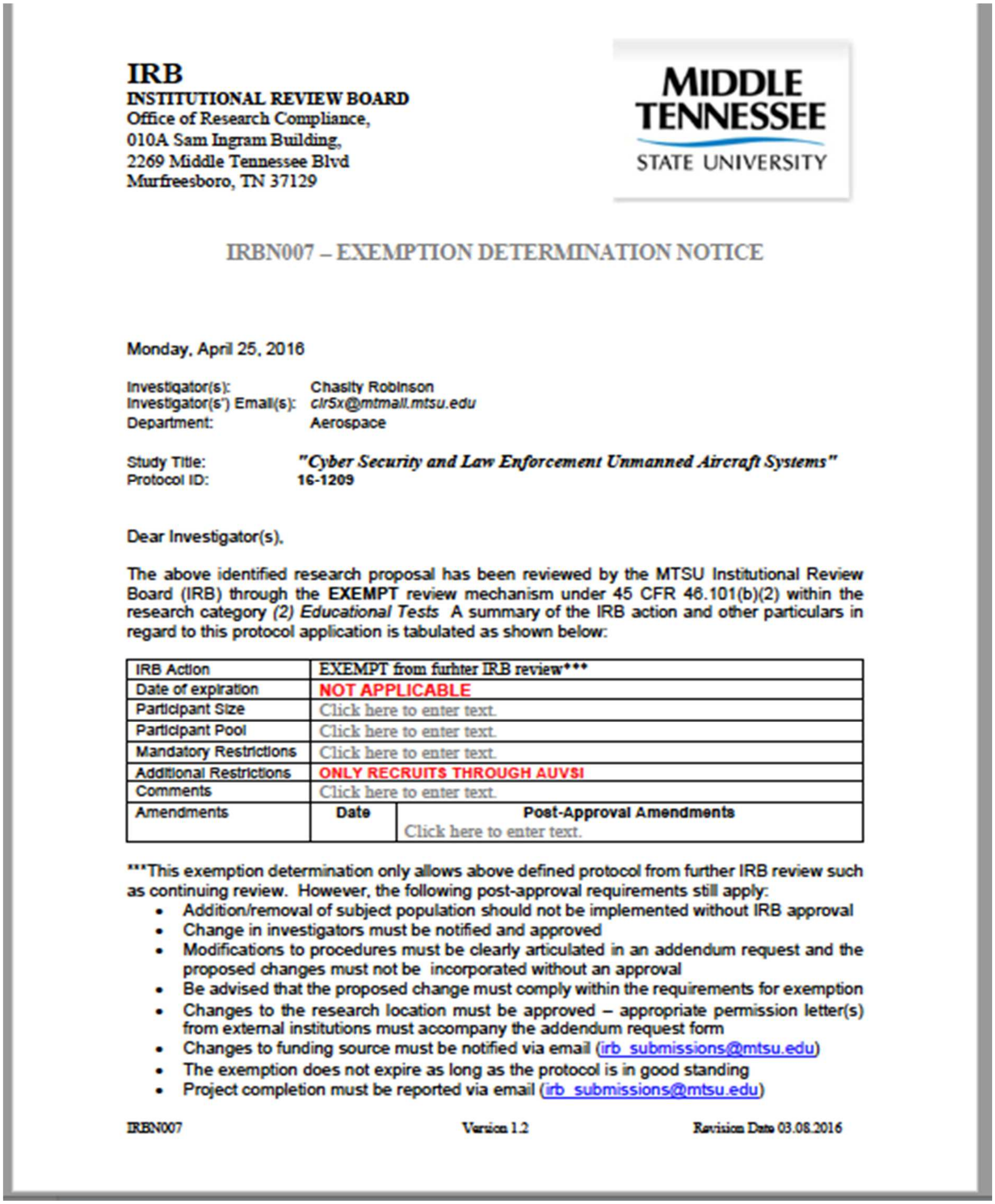
USLegal. (2016). Public safety law & legal definitions. *USLegal.* Retrieved from http://definitions.uslegal.com/p/public-safety/

Vervaeck, A. (2014). Earthquake in Ludian County (Yunnan), China-death toll increases further to 617 and +3143 people injured, just under $10 bn damage. *Earthquake-Report.com.* Retrieved from http://earthquake-report.com/2014/08/03/very-strong-earthquake-sichuan-yunnan-guizhou-rg-china-on-august-3-2014/

APPENDICES

APPENDIX A

Institutional Review Board Approval Letter



IRB
INSTITUTIONAL REVIEW BOARD
Office of Research Compliance,
010A Sam Ingram Building,
2269 Middle Tennessee Blvd
Murfreesboro, TN 37129

MIDDLE TENNESSEE
STATE UNIVERSITY

IRBN007 – EXEMPTION DETERMINATION NOTICE

Monday, April 25, 2016

Investigator(s):	Chasity Robinson
Investigator(s') Email(s):	*clr5x@mtmail.mtsu.edu*
Department:	Aerospace
Study Title:	***"Cyber Security and Law Enforcement Unmanned Aircraft Systems"***
Protocol ID:	**16-1209**

Dear Investigator(s),

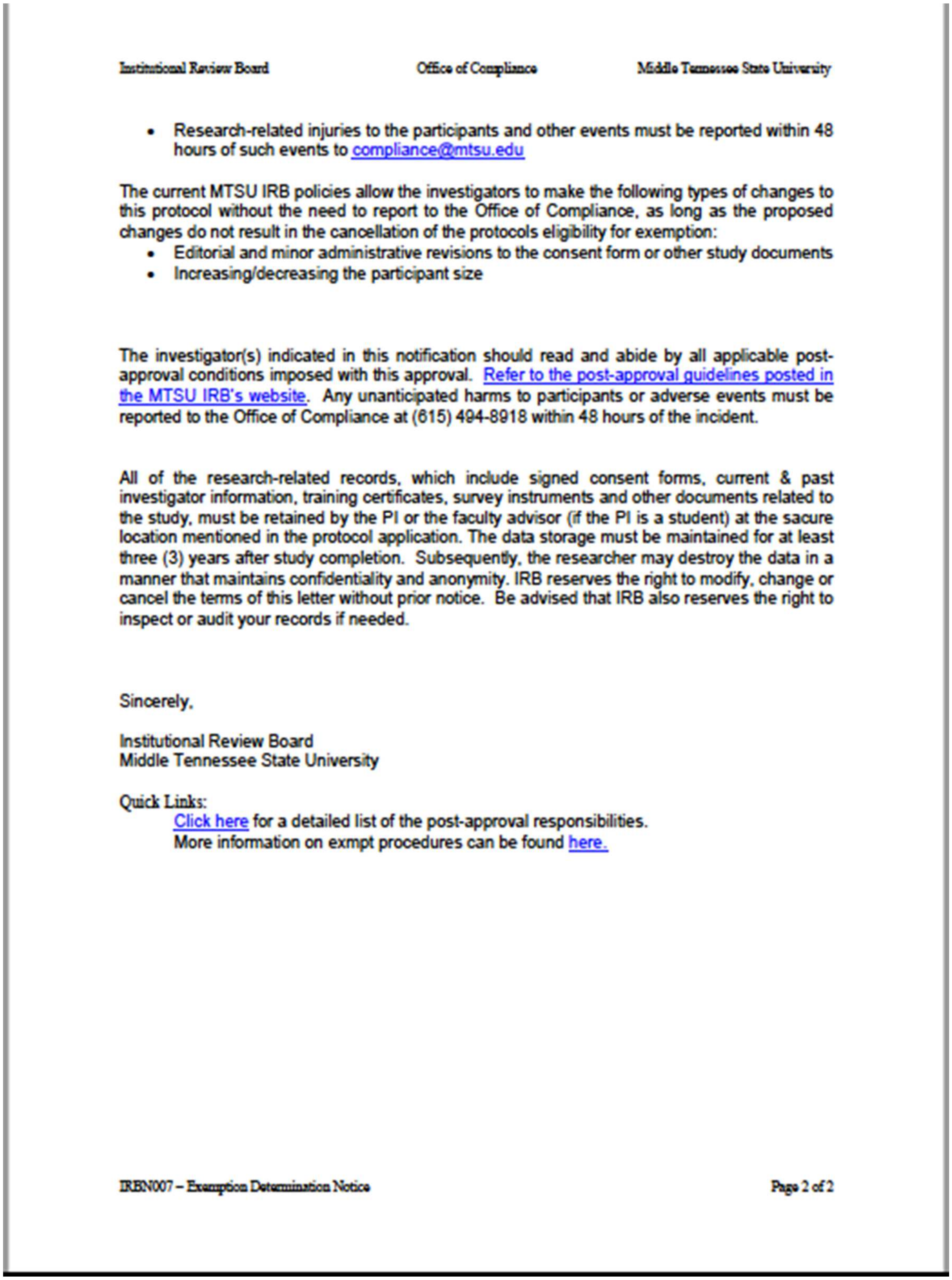
The above identified research proposal has been reviewed by the MTSU Institutional Review Board (IRB) through the **EXEMPT** review mechanism under 45 CFR 46.101(b)(2) within the research category *(2) Educational Tests* A summary of the IRB action and other particulars in regard to this protocol application is tabulated as shown below:

IRB Action	EXEMPT from furhter IRB review***	
Date of expiration	NOT APPLICABLE	
Participant Size	Click here to enter text.	
Participant Pool	Click here to enter text.	
Mandatory Restrictions	Click here to enter text.	
Additional Restrictions	ONLY RECRUITS THROUGH AUVSI	
Comments	Click here to enter text.	
Amendments	**Date**	**Post-Approval Amendments** Click here to enter text.

***This exemption determination only allows above defined protocol from further IRB review such as continuing review. However, the following post-approval requirements still apply:

- Addition/removal of subject population should not be implemented without IRB approval
- Change in investigators must be notified and approved
- Modifications to procedures must be clearly articulated in an addendum request and the proposed changes must not be incorporated without an approval
- Be advised that the proposed change must comply within the requirements for exemption
- Changes to the research location must be approved – appropriate permission letter(s) from external institutions must accompany the addendum request form
- Changes to funding source must be notified via email (irb_submissions@mtsu.edu)
- The exemption does not expire as long as the protocol is in good standing
- Project completion must be reported via email (irb_submissions@mtsu.edu)

IRBN007 Version 1.2 Revision Date 03.08.2016



- Research-related injuries to the participants and other events must be reported within 48 hours of such events to compliance@mtsu.edu

The current MTSU IRB policies allow the investigators to make the following types of changes to this protocol without the need to report to the Office of Compliance, as long as the proposed changes do not result in the cancellation of the protocols eligibility for exemption:

- Editorial and minor administrative revisions to the consent form or other study documents
- Increasing/decreasing the participant size

The investigator(s) indicated in this notification should read and abide by all applicable post-approval conditions imposed with this approval. Refer to the post-approval guidelines posted in the MTSU IRB's website. Any unanticipated harms to participants or adverse events must be reported to the Office of Compliance at (615) 494-8918 within 48 hours of the incident.

All of the research-related records, which include signed consent forms, current & past investigator information, training certificates, survey instruments and other documents related to the study, must be retained by the PI or the faculty advisor (if the PI is a student) at the sacure location mentioned in the protocol application. The data storage must be maintained for at least three (3) years after study completion. Subsequently, the researcher may destroy the data in a manner that maintains confidentiality and anonymity. IRB reserves the right to modify, change or cancel the terms of this letter without prior notice. Be advised that IRB also reserves the right to inspect or audit your records if needed.

Sincerely,

Institutional Review Board
Middle Tennessee State University

Quick Links:

Click here for a detailed list of the post-approval responsibilities.
More information on exmpt procedures can be found here.

APPENDIX B

Survey

Unmanned Aircraft Systems for Law Enforcement Survey

(Link to the survey: https://www.surveymonkey.com/r/lawenforcementuassurvey)

Greetings! Please take a few minutes to participate in this anonymous survey on Unmanned Aircraft Systems for Law Enforcement Departments. You will not be asked to provide any information regarding the identity of your Department or your identity. Participating in this project is voluntary, and refusal to participate or withdrawing from participation at any time during the project will involve no penalty or loss of benefits to which you might otherwise be entitled. All efforts, within reason, will be made to keep the personal information in your research record private but total privacy cannot be promised, for example, your information may be shared with the Middle Tennessee State University Institutional Review Board. In the event of questions or difficulties of any kind during or following participation, you may contact the Principal Investigator as indicated below. For additional information about giving consent or your rights as a participant in this study, please feel free to contact the MTSU Office of Compliance at (615) 494-8918.

Please note that you may withdrawal your participation at any time during the survey. Your feedback will remain anonymous and is highly appreciated and important!

Questions, comments, concerns? Contact: Chasity Robinson at clr5x@mtmail.mtsu.edu

By clicking the "NEXT" button you will have expressed consent to participate in the survey.

1. Approximately how long have you been working in Law Enforcement or assisting with Law Enforcement?

- o Less than 2 year
- o 2-5 years
- o 6-10 years
- o 11-15 years
- o 16-20 years
- o 21-24 years

- More than 25 years

2. Does your Law Enforcement Department utilize Unmanned Aircraft Systems or does the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems?

- Yes
- No

3. How often does your Law Enforcement Department or the Law Enforcement Department you assist with utilize Unmanned Aircraft Systems?

- Once per month
- Once per week
- 2-3 times per week
- More than 4 times per week
- Not sure

4. Have you been involved or assisted in a Law Enforcement Unmanned Aircraft Systems Department?

- Yes
- No

5. How much *total training* have you received for Unmanned Aircraft Systems operations?

- Less than a week
- 1-3 weeks
- 4-7 weeks
- 8-11 weeks
- More than 12 weeks
- 3-6 months

6. How much *total operational experience* have you received for Unmanned Aircraft Systems operations?

- Less than a month
- 1-3 months
- 4-7 months
- 8-11 months
- 1-2 years
- More than 2 years

7. What level of FAA training do you possess?

- Private Ground School
- Sport/Recreational Pilot Certificate
- Private Pilot Certificate

- Above Private Pilot Certificate (i.e. Instrument, Commercial, CFI)
- No FAA Flight Training

8. How effectively does the Unmanned Aircraft Systems seem to complete various tasks within your Law Enforcement Department or the Law Enforcement Department you assist with?

- Very effective
- Effective
- Neutral
- Very ineffective
- Not at all effective

9. Considering the control system (data link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?

- Very secure
- Secure
- Neutral
- Not very secure
- Not at all secure

10. Considering the image system (video link) of Unmanned Aircraft Systems, how secure do you think the Unmanned Aircraft Systems within your Law Enforcement Department or the Law Enforcement Department you assist are?

- Very secure
- Secure
- Neutral
- Not very secure
- Not at all secure

11. Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think it is that a person can hack into Unmanned Aircraft Systems during *operational* use?

- Very likely
- Likely
- Neutral
- Not very likely
- Not at all likely

12. Considering the current and future developments of Unmanned Aircraft Systems operations for Law Enforcement Departments, how likely do you think a

person can hack into Unmanned Aircraft Systems during *non-operational* use?

- Very likely
- Likely
- Neutral
- Not very likely
- Not at all likely

13. How likely do you think it is for a person who hacks into an Unmanned Aircraft Systems to pose harm for public safety?

- Very likely
- Likely
- Neutral
- Not very likely
- Not at all likely

14. What are some security risk concerns you have for the use of Unmanned Aircraft Systems for Law Enforcement Departments that may affect public safety?

15. What are some preventive cyber hacking measures your Department or Law Enforcement Department implements on Unmanned Aircraft Systems?