CYBER THREATS TO CIVIL AVIATION

by

Kerri A. Heitner

A Capstone Project Submitted to the Faculty of

Utica College

[Month and Year approved by your committee]

in Partial Fulfillment of the Requirements for the Degree of

Master of Science in Cybersecurity

© Copyright 2014 by Kerri A. Heitner

All Rights Reserved

**Abstract**

**REQUIRED** – Start abstract text here. Notes about formatting are included throughout this template, but you are responsible for ensuring that all requirements included in the Formatting and Submission Guide are met. Please note that this template is already set up with the correct margins, paginations, and justifications. Be careful not to delete page breaks or section breaks at the bottom pages – to see them, click on the ¶ icon at the top of your Word document (stands for “show all nonprinting characters”). The abstract is a concise summary of the research. It should describe the purpose, importance, results, and conclusions of the research. The abstract is to be written in a scholarly manner. The abstract must be at minimum 220 words, but not exceed one page in length, including keywords. The last sentence of the abstract must start with the word “Keywords:” followed by the academic program [select appropriate academic program and include *as written here*: Criminal Justice Administration, Cybersecurity, Economic Crime Management, Education, Health Care Administration, Liberal Studies, Occupational Therapy, Physical Therapy], thesis/capstone project adviser’s full name, and **up to five additional keywords that are not included anywhere else in the abstract**. Example of last sentence: Keywords: Liberal Studies, Dr. Polly Smith, sociological, anthropological, social, qualitative, human rights.

Here is a good link for information about writing an abstract:

<http://psychology.about.com/od/apastyle/ht/abstract.htm>

**Acknowledgements**

OPTIONAL – Insert your acknowledgements text here or delete this page, including the page break at the bottom of the page. The acknowledgments are personal for the student and may contain appropriate information, written in a professional manner, that the student may wish to share with the reader. Please note that this information will be on the World Wide Web for any person in the world to view. There is no word limit, but the acknowledgments must not exceed one page in length. Any quotes listed in this section need to be cited; however, use of copyrighted material in this section is discouraged. Pagination began on the Copyright page with Roman numeral ii; pagination on this page continues sequentially using Roman numerals.

**Table of Contents**

[REQUIRED – Insert your Table of Contents here. The text for the table of contents must be single-spaced (double-spaced from the page header) in Times New Roman font, 12-point size, black. The table of contents does not include any pages prior to or including the Table of Contents page. Example:]

**Use Word to do your TOC, it will do it cleaner and neater than doing it yourself.**

List of Illustrative Materials vi

Level One Heading – Section One 1

Level Two Heading 2

Level three heading 2

Level four heading 2

Level five heading 2

Level One Heading – Section Two 2

Level Two Heading 2

Level three heading 2

Level Two Heading 2

Level three heading 2

Level One Heading – Section Three 2

Level One Heading – Section Four 2

Level One Heading – Section Five 2

References 3

Appendices 4

Appendix A – Title 5

Appendix B – Title 5

**List of Illustrative Materials**

[OPTIONAL – Insert your List of Illustrative Materials here, if applicable. Illustrative materials include tables, graphs, charts, figures, photographs, and other illustrations. The term "Table" is used to designate tabulated data; this includes computer printout sheets. The term "Figure" is used to designate photographs, half-tone prints, charts, maps, graphs, plates, drawings, diagrams, and other mainly nonverbal material. The text for the list of illustrative materials must be single-spaced (double-spaced from the page header) in Times New Roman font, 12-point size, black. Tables and Figures should be listed in chronological order as they appear in the paper. If you do not have illustrative materials in your thesis or capstone project, remove this page by backspacing. DO NOT delete the section break at the bottom of this page, or the page number format will be changed! Example:]

Table 1 – Title 2

Figure 2 – Title 2

Table 3 – Title 2

**Cyber Threats to Civil Aviation**

Civil aviation security policies present detailed information about physical security measures and procedures, but lack any standard policies regarding cybersecurity. There are an increasing number of cyber threats to civil aviation systems without proper mitigation techniques and implemented policies to counter potential attacks. One reason why civil aviation has become one of the most successful and a reliable form of transportation is due to a very precise set of international standards implemented by the International Civil Aviation Organization (ICAO). These standards include English as the universal language with frequent proficiency tests to prevent miscommunication errors in-flight (ICAO, 2011). The same diligence must be practiced to create a standard for cyber related security breaches and threat mitigation.

The purpose of this research was to create an awareness of aircraft system vulnerabilities in order to provoke change among current international cybersecurity policies, procedures and standards. This project intended to answer the following questions: What are the cyber threats to Automated Dependent Surveillance-B (ADS-B) systems of an aircraft in-flight? What are the cyber threats to Aircraft Communications Addressing and Reporting Systems (ACARS) of an aircraft in-flight? What are the vulnerabilities from insider threats to cybersecurity? How does the lack of a cybersecurity plan affect Electronic Flight Bags (EFB)? What is the aviation industry's response to the issue of cybersecurity and in-flight safety?

Cyber security has been identified as a high-level impediment to the implementation of the Global Air Navigation Plan. The term "cyber security" encompasses the protection of electronic systems from malicious electronic attack and the means of dealing with the consequences of such attacks. It compromises managerial, operational and technical activities, and relates to the electronic systems themselves and to the information held and processed by such systems. Currently cyber security is a relatively minor issue in civil aviation but this is changing. New technologies are being adopted which are intrinsically more vulnerable to cyber attack and which collectively increase the impact from such attacks. (International Civil Aviation Organization, 2012, p. 1)

As interconnectivity increases, security must also increase for the critical computer networks set up to fly an aircraft and communicate with ground stations. In the civil aviation industry, the trend since the 9/11 terrorist attacks has been to increase physical security measures. This has proven very effective. However, with the daily technological advancements in computer systems widely used to operate aircraft, the aviation industry must be proactive in setting new standards for cybersecurity (Iasiello, 2013).

Cyber security policies regarding in-flight aircraft systems present a unique challenge because the networks depend heavily on ADS-B. ADS-B is an essential part of Next Generation Air Transportation (NextGen): a new way of managing aircraft controls. NextGen is the switch from radar to satellite technology in directing air traffic **(Federal Aviation Administration, 2013)**. By 2020, NextGen is expected to be fully implemented in the United States in addition to many other countries around the world. Contrary to most critical infrastructure that is vulnerable to cyber-attacks due to outdated legacy computer operating systems; ADS-B is a brand new system. Experts question why this system is said to be lacking the necessary encryption and authentication. This could mean potential attackers spying on or spoofing communications **(Greenberg, 2012).**

When network systems lack cryptographic algorithms, the network remains vulnerable for an attacker to gain full access of the ADS-B wireless channel. As a result, messages can be falsely entered, manipulated or permanently removed as either a passive or active attack. Passive attacks could include methods of eavesdropping in which an attacker could gather the information for a greater plan. "Since ADS-B messages are not encrypted, they can be recorded and misused to obtain unique identifiers of aircraft as well as accurate position trajectories" **(International Civil Aviation, 2014, p. ?).** Attackers could use ADS-B receivers and open-source information on the Internet to collect and analyze data on ADS-B traffic **(International Civil Aviation, 2014).**

Active attacks pose more of an immediate threat as they include "attacks on air traffic monitors and automated assisting systems like collision avoidance (TCAS) and pilots" **(International Civil Aviation, 2014, p. ?).** Active attacks would be any type of manipulation to the ADS-B wireless channel, including ghosting and deletion of aircraft. Ghost Aircraft Injection could cause safety threats to nearby aircraft and cities. If an attacker creates or deletes one or multiple spoofed aircraft on the radar, it could cause confusion and chaos at an air traffic control center. Ghost Aircraft Injection can be especially problematic during crucial times such as take-off and landing. This confusion could create unsafe conditions and misinformed decisions from controllers. Another possibility is Ghost Aircraft Flooding which could cause a denial of service (DoS) where ATC would be unable to function properly as a result of overloading the wireless channel **(International Civil Aviation, 2014).**

An additional threat to ADS-B to consider is the reliance of satellite or GPS to function. "Several incidents have demonstrated that GPS has been subject to intentional and unintentional targeting and disruption by both state and non-state actors" **(Iasiello, 2013, p.?).** GPS has proven to be unreliable when civilians using jammers have unintentionally interfered with ATC. Intentional events regarding GPS hijacking have also been reported in the past. Hackers can manipulate satellite transmission by gaining network access to a ground station (Iasiello, 2013).

The Federal Aviation Administration (FAA) assures that ADS-B is able to determine and rule out any fictitious signals using multilateration (MLAT) confirmed by radar. MLAT was created from the extrapolation of air traffic doubling by 2025. This new system would allow for more planes to operate safely in the sky. It was advisable for the FAA to upgrade from radar because Secondary Surveillance Radar (SSR) was developed over 60 years ago and was not equipped to handle advancements in today's technology. Although SSR is updated every 4-12 seconds with verified signal replies, it was not good enough to keep it around. The concerns over future technological advancement support and coverage interference from high terrain were too risky **(ERA Corporation, 2014).**

An advantage of ADS-B is increased aircraft status updates at once per second. Information included in these updates is projected path, speed, altitude, velocity and aircraft identificationalong with other pertinent information. Instead of sending out a signal and waiting for a returned response, ADS-B utilizes satellites for the recognition of aircraft. The aircraft is constantly broadcasting its information for the satellites to pick up and transmit to air traffic control stations. In turn, the air traffic control stations can also send helpful information, such as weather updates, to the crew of an aircraft without speaking it over voice controls **(ERA Corporation, 2014).** Ultimately, ADS-B is a consistent flow of readily available information, as opposed to a broken up question and answer style of information gathering used in radar. Comparably, it as if aircraft were switched from a dial up modem to broadband cable.

As it has been observed in the past, the more readily available and convenient information is, the higher the risk of the information being compromised. The problem with this solution is the reported malfunctions with the software and hardware that is used for NextGen **(Iasiello, 2013).** Commercial Off-The-Shelf (COTS) technology was created to be easily added to existing systems, while never needing services or labor intensive customization. By standardizing system functions, COTS is customary in the public sector because it is inexpensive to create and maintain **(Pregasis, 2014).** In turn, standardization equates to less custom engineering and an increased risk for cyber attack.

COTS software in the aviation industry is developed overseas and used without the knowledge of a source or application code. Since there is no ownership for COTS and the source code cannot be accessed, conventional methods of analysis would not produce desirable results. This has led to malicious activity such as embedding hidden functions into the software because there is no way to detect alterations. The COTS systems that are used for NextGen are vulnerable to manipulation. Although the purpose of COTS was for security purposes, implementation is risky and could lead to serious malfunctions within aviation network systems. Specifically, cockpit IT systems that rely on COTS for general internet protocols such as wireless access when on the ground and satellite networks in flight. Wireless access is already considered unreliable and prone to signal intereferences. Specifically, cockpit IT systems that rely on COTS for general internet protocols such as wireless access when on the ground and satellite networks in flight. Wireless access is already considered unreliable and prone to signal interruptions and/or manipulations. Cockpit systems rely o COTS *and* wireless access, which puts a double threat on the critical functions carried out by pilots (Iasiello, 2013).

The ICAO held a meeting in April 2014 regarding security issues of ADS-B operations. The organization references the Aviation Security Manual Doc 8973/8, "states have been urged to include provisions for protection of critical information and communication technology systems against cyber-attacks and interference" **(International Civil Aviation Organization, 2014, p.?).** Another reference to the ICAO Air Traffic Management Security Manual Doc 9985 AN/492 First Edition - 2013 included the statement that "emphasis has been laid on protection of Air Traffic Management Systems against cyber-attacks" **(International Civil Aviation Organization, 2014).** These warnings and recommendations became more crucial as ADS-B was exposed for being extremely vulnerable to cyber attacks. The ICAO referenced the independent researchers who have published papers looking to make the aviation industry more aware of the risks involved with ADS-B. The ICAO urges that a mitigation policy be formed on the potential ADS-B security problems and uniformly implemented across the United States **(International Civil Aviation Organization, 2014).**

Considering that a prime component to aircraft safety such as ADS-B is not regulated by cybersecurity standards is a prime example for why an immediate change is needed in the civil aviation industry. The definition of cyber terrorism in civil aviation according to the United States is "acts of unlawful interference… politically or otherwise motivated use of violence directed at civilians by a group or individual in order to influence public perceptions" **(Whiteman, 2001, p.74).** The definition in Canada is "actions taken in support of national objectives which influence decision-makers by affecting others' information while exploiting and protecting one's own information" **(Whiteman, 2001, p.74).** The discrepancy between these two definitions is a problem because neither is fully accurate. If countries cannot come to an agreement on defining the problem; they cannot implement a working mitigation policy.

When exploring the success of existing physical security standards and procedures, it is apparent that there is a growing need for a national and international cybersecurity policy. The safety of aircraft and its passengers, along with any target that could be potentially part of a grander terrorist plot is at high risk without adequate cyber threat mitigation techniques. Although many of the studies discussed in this paper have had arguments made against the likelihood of occurrence, it should be noted that "the absence of evidence does not equate to the absence of threat" **(Iasiello, 2013, p?).**

State and non-state actors could already be dedicated to creating methods for taking control of an aircraft in-flight. Some experts believe there is a possibility that this may have already happened. With consideration of recent events, it would not be wise to completely rule out the chance that Malaysian Airlines Flight MH370 was a cyber attack in some form. The disappearance of MH370 traveling from Kuala Lumpur International Airport to Beijing Capital International Airport on March 8, 2014 has become a big controversy for over six months as the aircraft sent its last ACARS message to ATC less than an hour after takeoff (BBC News, 2014).

A more plausible explanation of an attack this sophisticated is that it originated as an insider threat. Most likely, if this were a cyber attack, the persons responsible would have been extremely knowledgeable on aircraft system engineering. The most indicative aspect of this unsolved investigation is that the aircraft communication was shut down completely, which investigators believe to be intentional. In order for all communication with radar and air traffic control to be silenced, an aircraft such as MH370 which was a Boeing 777, a three step process would have had to be performed (Paganini, 2014).

Boeing 777 uses many transponders to communicate their position to air traffic control. It is not simple to switch off all the transponders, and modern planes, in fact are equipped with two other systems, the cockpit radio and a text-based system known as Aircraft Communications Addressing and Reporting Systems (ACARS), which can be used to send messages or information about the airplane. **(Paganini, 2014, p. ?)**

The point of this research was not to prove or disprove the likelihood of Malaysian flight MH370 as a cyber attack. However, the importance of such an event is that it raises awareness to all potential mitigation techniques. It is possible for a cyber attack to have the capabilities presented in this devastating loss. Therefore, vulnerabilities in all scenarios must be considered.

The present state of cyber policies in aviation is non-existent. There is a direct correlation of increased safety and success among physical security standards, yet cybersecurity is not properly addressed. Several studies support many facets of information that can be accessed and manipulated without a working cybersecurity policy. These include but are not limited to forfeiting access to in flight controls, manifest and banned lists, air traffic control manipulation, ghosting and communication interference.

**Literature Review**

**ADS-B**

The transition from SSR to ADS-B was derived from the aviation industry striving to improve upon traffic awareness. ADS-B is the key component to the NextGen software that The FAA has made a mandatory requirement of all aircraft by December 31, 2019. An advantage of switching to ADS-B is that GPS positions are more accurate and consistent than radar, which allows for more air traffic with closer spaced aircraft than existing procedures allow for ("ADS-B", n.d.).

Another aspect that has induced the switch to ADS-B is that it allows for communication from aircraft to another nearby aircraft, as well as to ATC. For now, The FAA is only requiring ADS-B "Out" feature for the December 31, 2019 mandate. This means that it is sending its position to ATC. The feature that it can communicate and receive location from other nearby aircraft will remain an optional feature at this time. Although the deadline to install the ADS-B requirements is December 31, 2019, most US aircraft are already considered fully prepared for the change. It is noted that Europe, Australia and Fiji have functioning existing ADS-B programs ("ADS-B," n.d.).

In order for ADS-B to function, aircraft must have a GPS receiver to determine its location and a data link transmitter to send out the position. International standards for ADS-B "Out" require a Mode S transponder that uses an Extended Squitter (ES) to transmit messages on 1090 Megahertz (MHz) frequency. This method of communication is also referred to as 1090 ES. The GPS receiver must be Instrument Flight Rules (IFR) certified which is regulated by ATC ("ADS-B", n.d; Stoen, 2000).

ADS-B In is the optional feature which allows for the aircraft to receive position reports from nearby aircraft, without ATC acting as a liaison. This is also referred to as Cockpit Display of Traffic Information (CDTI) ("ADS-B", n.d.). CDTI "is a self-extracting Win-Zip file that is password protected... in beta form and will not be generically available until further testing and development" (CDTI, 2009, page/para??).

ADS-B is also capable of in-flight weather updates. When paired with an iPad and the ForeFlight application, pilots can have a more detailed view of their flight path respective of weather and other aircraft (Stratus 2, n.d.) The weather application should be used for long-term strategy as opposed to short-term navigation through storms. However, it proves to be very useful when creating a flight plan ("ADS-B weather products", 2013).

**ACARS**

ACARS is the international communication infrastructure that many airlines use for air-to-ground data transmission of ATC and Airline Operational Control (AOC). ACARS functions by the use of VHF and HF satellite communications and ground stations in which it sends and receives billions of messages a year. ACARS can operate differently depending on where an aircraft is and what it is equipped with.

AOC messages include take-off and landing confirmation, weather information, gate information, and engine reports. ATC messages include navigation information, aircraft positional reporting, departure clearances, oceanic clearances, runway conditions, and weather data. Currently AOC messages take up 80% of ACARS network traffic versus 20% for ATC, but the FAA NextGen program will shift more and more voice communications to data in the near future. **(ARINC, n.d., para 3)**

ACARS acts as an aid to the flight crew by using computer technology to send and receive routine messages and reports. ACARS uses the same VHF radio that is used for voice communication and can be monitored with a VHF scanner on the aircraft band 118 to 136 MHz. The standard frequency for the US is 131.550 MHz **(ACARS WEB-FIREFOX FAVS).** When aircraft are flying over land, VDLM2 is used to route and deliver ACARS communication through a network of VHF stations. VDLM2 is ten times faster than traditional VHF. Over large bodies of water such as the ocean, ACARS data is transmitted through Inmarsat satellite communications, Iridium satellite communications or HFDL ground stations (ACARS ARINC).

**Vulnerabilities in ADS-B and ACARS**

After the release of the new hardware and software needed to carry out the functions of NextGen, many people including hackers and security experts began questioning the security of the new system. The simplest form of a security breach to ADS-B is eavesdropping. This is the when someone listens to broadcast transmissions that are unsecure. Aircraft Reconnaissance refers to the passive attack performed while eavesdropping. Developers were aware of the potential for eavesdropping since they started to create ADS-B. Although eavesdropping alone is fairly harmless, it is the foundation for more sophisticated attacks. Without full encryption, eavesdropping is very difficult to prevent and nearly impossible to discover upon execution. (Strohmeier, Lenders, & Martinovic, 2014, pg. 4).

Another simple form of breaching ADS-B security is jamming. Jamming affects either an aircraft or ground station and disables the ability to send and receive messages. This is done when someone uses high power on Mode S of the 1090 MHz frequency. Jamming aviation communication is especially problematic because of "the system's inherent wide open spaces which are impossible to control as well as the importance and criticality of the transmitted data"(Strohmeier et al., 2014, p.3). ADS-B receivers are typically difficult to blackout in any given area, however, it can be done and a targeted attack on such systems would result in "major denial-of-service problems at any airport". Ground Station Flood Denial and Aircraft Flood Denial are prime examples of jamming attacks (Strohmeier et al., 2014, p.4).

Message injection, deletion and modification are the moderately to extremely difficult ADS-B exploits, in that order, depending on specific circumstances. Message injection includes false messages planted in the air-traffic communication system. This is possible due to the lack of authentication of ADS-B messages at the data link layer. This allows attackers to build and use a transmitter for spoofed ADS-B messages with ease. Without authentication, there is no liability and this can result in confusion between ATC and pilots over legitimacy discrepancies. Aircraft/Ground Station Target Ghosts Injection and Flooding are prime examples of message injection attacks(Strohmeier et al., 2014).

Message deletion can be performed wirelessly by destructive or constructive interference. Destructive interference is "transmitting the inverse of the signal broadcast by a legitimate sender"((Strohmeier et al., 201, pg. 4). This method is difficult because of superposition and the particular timing requirements which increase the probability of failure. Constructive interference does not rely on strict timing requirements which allows for a higher success rate with enough errors to prove useful. Mode S extended squitters' CRC corrects at most five bit errors each message. If a message has more than five, it will drop the message and mark it corrupted. Unlike destructive interference, constructive interference will usually result with the receiver being able to verify that a message was sent. Both methods are less abrasive than completely jamming 1090MHz frequency. A prime example of a message deletion attack is Aircraft Disappearance (Strohmeier et al., 2014).

Message modification is the most difficult of the ADS-B exploits. It is executed during transmission at the physical layer through bit-flipping or overshadowing. Bit-flipping is the "attacker superimposing the signal converting any number of bits from 1 to 0". Overshadowing is when an attacker replaces all or part of a message by sending a high-powered signal. Both methods can be performed without the user's knowledge. Message modification is ultimately comprised of message deletion and message injection. These two methods could be combined to gain a similar outcome. However, physical layer message modification is considered more threatening because the manipulation came from an originally legitimate message. Prime examples of message modification include Virtual Trajectory Modification and Virtual Aircraft Hijacking (Strohmeier et al., 2014).

German commercial pilot and computer security expert, Hugo Teso, has been researching aviation security since 2010. Teso first presented the vulnerabilities in ADS-B and ACARS to the aviation industry at the annual Hack in the Box security conference in 2013 in Amsterdam. Teso presented an Android application, PlaneSploit, to gain control over an aircraft remotely. He was able to exploit vulnerabilities in the ACARS and ADS-B functions by using free source software and websites to gather necessary tools and information **(Croft, 2013\*FROM ORIGINAL PAPER).** Teso acquired hardware from eBay, which he noted was very easy and affordable. These included Honeywell aircraft management units and simulation tools with aircraft code **(Adhikari, 2013).** Teso stated that eBay is not the only place that aircraft hardware and software can be found for sale. They can also be found through aircraft product vendors who are eager to sell, third party vendors with less security, and from resentful prior employees **(YOUTUBE TESO**).

With the aid of these tools, Teso was able to create a virtual FMS in which he could manipulate flight plans and attain GPS coordinates of nearby aircraft. Public websites such as flightradar24.com allowed Teso to track flights in real-time from ADS-B. These websites give detailed information about the aircraft model, make, carrier, registration number, altitude, speed and departure and arrival times. Teso used the ADS-B open source data to determine which model FMS a specific aircraft was using, this was another key component to his simulated experiment (Adhikari, 2013).

Figure 1 displays how easily the information of a flight path and aircraft is to obtain on flightradar24.com. At random, one of the planes shown was selected. This aircraft is a Boeing 767, operated by American Airlines and was traveling from Miami, Florida to Paris, France. It shows the flight plan and details about the aircraft registration. More information can be displayed when scrolling after the registration. Teso would have compared Boeing 767 under American Airlines to online research to find which FMS is commonly used on this particular aircraft and airline. Detailed information such as preferred flight paths and cruising altitude speed could be carefully collected upon dedicated observation of specific routes. ADS-B data in real time was displayed in yellow, with FAA data in orange and five minutes delayed.



Figure 1 Flight Tracker http://www.flightradar24.com/AAL62/49269ba

When manipulating ACARS, Teso found that many messages were not encrypted or secure. By passively eavesdropping to gather information, he was able to replay, jam and complete signal injections (CYBERARMS, BOOKMARK). The main goal of Teso's experiment was to exploit the aircraft FMS using ACARS. He was able to upload false FMS data through Software Defined Radio (SDR) and Ground Service Providers **(YOUTUBE,TESO).** Teso believes that a cyber-hijacking could be accomplished through the application he created. PlaneSploit would allow someone on the ground to send spoofed commands to a specific aircraft as long as it was using the autopilot. The different functions that Teso manipulated included speed, altitude, direction, and even control over lights inside the cabin. Teso stated that the light functions could be used as a way of terrorizing passengers and flight crew on board by repeatedly turning the cabin lights on and off in-flight to cause panic. (YOUTUBE).

Teso was not the only computer expert to release ADS-B vulnerabilities. At Black Hat, a convention of computer hackers and computer security personnel, in Las Vegas in 2012, Andrei Costin claimed that anyone with decent computer technology skills and around $2,000 worth of electronic equipment could manipulate ATC or locate a celebrity private jet. Costin claimed that ADS-B has no verification process when receiving messages. Due to this security flaw, hackers are able to easily impersonate another aircraft sending messages. Even if ATC is wary of a message origin, the only way they can investigate its validity is by cross-checking flight plans, which is time consuming and would create unusable areas of air space until resolved. Costin warns that spoofed planes or ghosting can overload the FMS and there are not enough workers to cross-check if an attacker were to inject an unusually large amount of aircraft. This would create "a human resource version of a denial of service attack on an airport" **("Global air control" 2012, paragraph 6).**

Indirectly supporting Teso's experiment, Costin stated that NextGen broadcasts aircraft velocity, position and other pertinent information that is not encrypted. This results in the ability for an attacker to build or buy a device to capture this information from aircraft. Costin's presentation at Black Hat demonstrated the identification of Air Force One by picking it up from another aircraft broadcasting it. He then was able to execute the flight plan on an iPad. Costin was baffled that an aircraft as high profile as Air Force One would be broadcasted to other aircraft. Costin believes the readily available public information such as aircraft registration numbers is a significant factor to the displayed vulnerabilities at Black Hat **("Global air control" 2012)**.

Phil Polstra, associate professor of digital forensics at Bloomsburg University of Pennsylvania, spoke at DefCon 22 in July 2014. In response to Teso’s presentation at Hack in the Box 2012, he argued that it was not possible to cyberhijack an airplane. He referenced the findings in Teso’s research that rely on the autopilot function to hijack the plane. He claimed that it is more feasible to create mischief rather than take full control of the aircraft. Polstra said that pilots would notice if the controls were being manipulated and would turn off the autopilot. “All aircraft feature unhackable mechanical backup instruments” (Greenberg, 2014, para 3).

Polstra reported that avionics networks are not connected to Wi-Fi or entertainment and are never wireless. Refuting theories by researchers like Teso, Polstra argued that someone could not send malicious packets to the Ethernet ARINC 664 system and that the critical functions of an aircraft remain separate from functional networks for passengers. Polstra stated that it is possible to compromise ACARS by modifying or creating new flight plans and tampering with weather reports. During the presentation, Polstra’s partner speaker played a video of actors playing pilots who were communicating with ATC after suspicious messages were received. The video ends with the pilots ignoring ACARS as a result of their successful communication with ATC concerning the false messages. Polstra took a strict standpoint and makes fun of cyber hijacking with this video. In the same presentation, he admitted that ADS-B can be jammed with ghost planes and false weather updates. He also verified that almost every protocol in aviation is unencrypted. Even after these admissions, he remained confident that air travel is very safe and the disruptions that are possible would result in nothing more than an annoyance to ATC and pilots (Greenberg, 2014).

Brad Haines is a Certified Information Systems Security Professional (CISSP), also known as Renderman. He believes that aircraft tracking websites and applications that use ADS-B capabilities to give public information about individual aircraft are a threat to the cybersecurity of modern air travel. Haines presented his research at Defcon 20 in July 2012 (Haines, 2012). Defcon is the largest and longest running underground hacking conference in the world **(DEFCON, n.d).** Haines points out that ADS-B messages looks very similar to standard network packets and that this would be simple to hack (Haines, 2012). Figure 2 shows the comparability of the ADS-B Out data block to a network packet you would find in a common PC. The common foundation of the two packets could lead to computer savvy individuals recreating ADS-B messages for spoofing without any suspicion from ATC or the flight crew.

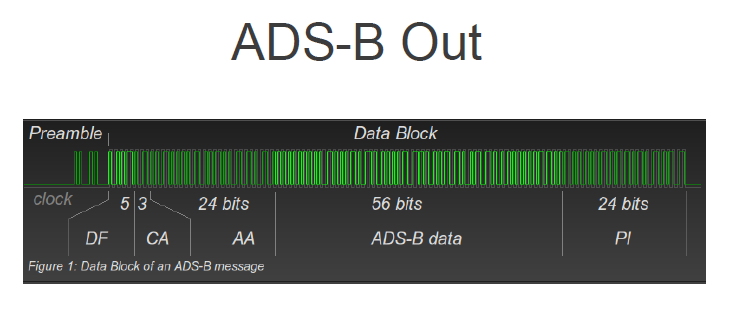


Figure 2 ADS--B Out

Haines reports that ADS-B is neither authenticated nor encrypted. He also mentioned that 1090MHz can be listened to by anyone, leading to the breakdown of messages from aircraft in real time. Haines admitted to monitoring all air traffic arriving and departing from Edmonton by running a ground station at his home. This research was done with good intentions as Haines claims he was trying to prove himself wrong about the cybersecurity flaws of aircraft network systems. To his disappointment, he could not disprove his original theory. Haines' main goal was to feel better about flying as he uses air travel frequently **(Haines, 2012).**

Haines states that there has yet to be any concrete security answers in response to the speculations surrounding NextGen's ability to withstand a cyber attack. He lists the threats of ADS-B Out as eavesdropping ADS-B messages, ghost injection and jamming of ATC reception. ADS-B In threats include data injection into ADS-B displays, aircraft GPS jamming and GPS spoofing or manipulation of coordinates. These threats have a wide range of results if executed ranging from a minor inconvenience to the flight crew or ATC to a major disturbance in flight plans and in the worst case scenario; a collision (Haines, 2012).

Haines claimed that a USB TV tuner that can be purchased for twenty dollars is capable of being made into an SDR where someone could receive ADS-B messages. He and Nick Foster, colleague and fellow computer hacker, presented a simulation of California airspace where they spoofed a fake aircraft by transmitting its signal on the standard frequency (Thurber, 2012). Haines and Foster were able to produce random packets, in which they felt anyone with moderate computer knowledge could easily do. They tested messages at 900MHz and video at 1090MHz. Haines believes flight plans are at risk and could be tampered with upon an upload from ATC to the aircraft in-flight. Although aircraft are very complex, when learning about one system, it is easy to interpret the information and apply it to others as they are closely integrated.

An article, published a few months after the release of Haines information at DEFCON in July of 2012, explained in detail how to track aircraft for less than twenty dollars. The researcher uses the name Argilo and used the TV tuner Haines spoke about, to receive ADS-B messages and fed the information into the Internet application Google Earth. According to Argilo, the tuner must be a Realtek RTL2832U chip with a wide range of frequencies; 64 to 1700MHz. Argilo purchased the tuner from the website Aliexpress for twenty dollars. Argilo then used Ubuntu Desktop12.04 LTS (a free Linux based operating system), 64-bit version to download and install GNU Radio through command line (Argilo, 2012).

GNU Radio is a free and open-source software development toolkit that provides signal processing blocks to implement software radios. It can be used with readily-available low-cost external RF hardware to create software-defined radios, or without hardware in a simulation-like environment. (**GNU Radio, n.d, paragraph 1**)

After installing the GNU onto Ubuntu, Argilo instructs the user to use command line prompts to download and install gr-air-modes. This software will be able to decode the ADS-S messages from aircraft. After plugging in the TV tuner, the user must enter a command prompt to ensure that the ADS-B traffic can be received. Argilo shows the output that indicates that the TV tuner is working correctly and advises that the user will see GPS coordinates and altitudes almost immediately. Algiro suggests that downloading Google Earth is an easier way to view the data once the information from the GNU is set to write its output to a KML file (Google Earth's file format). This process is also done by command line prompts. Figure 3 displays Algiro's research after the steps that were previously described. It is Air Canada Flight 839 making the final descent for landing, while also showing nearby aircraft.

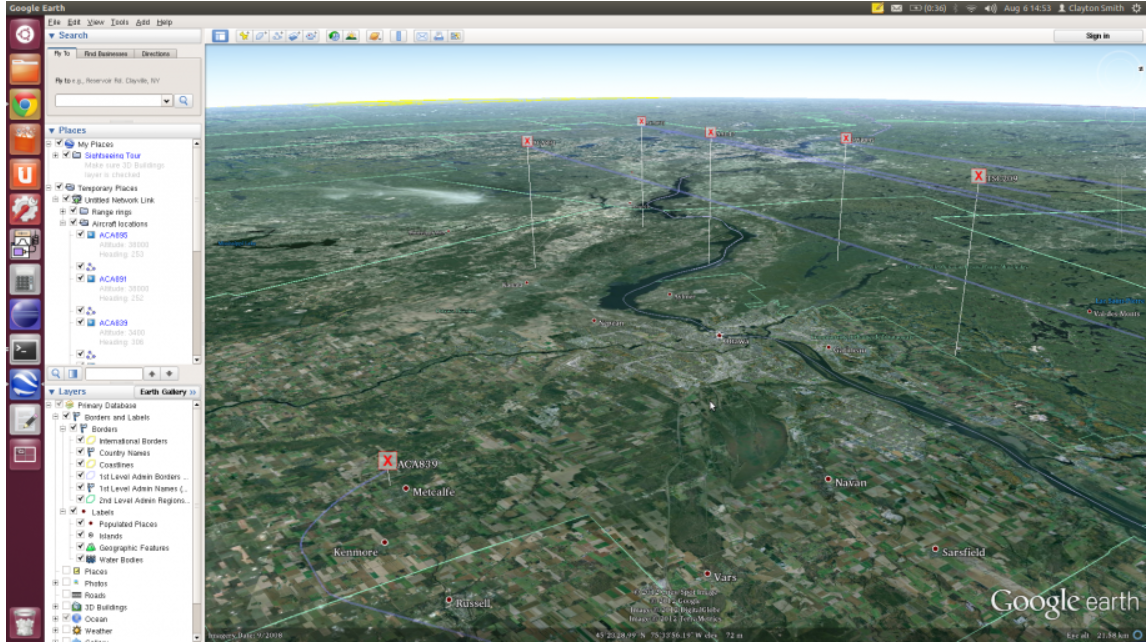


Figure 3 Air Canada Google Earth

On August 3, 2012 the FAA reported harmful interferences during a testing of Ground Based Augmentation System (GBAS) which incorporates ADS-B capabilities. GBAS increases navigation functions and signals of an aircraft approaching, departing or taxing to and from terminal areas. GPS jammers are strictly prohibited in the United States. There have been limited circumstances in which the use of GPS jammers was authorized under strict requirements and procedures, however this particular complaint had not been approved for official use (Federal Communications Commission, 2012).

On August 4, 2012, the FCC located the source of the reported interference of Newark Liberty International Airport GPS landing system. Gary Bojczak had been driving his employer’s pickup truck with a GPS jammer. His intention was to remain undetected from his employer as the trucks at his company were equipped to be tracked by management. GPS jammers are commonly bought by employee’s wishing to hide their daily routes and arrival times to jobs. It had been an ongoing problem as many truckers drive on the New Jersey Turnpike which is adjacent to the airport (Brewin, 2013; Federal Communications Commission, 2012).

Signal jammers operate by transmitting radio signals that overpower, jam, or interfere with authorized communications. While these devices have been marketed with increasing frequency over the Internet, with limited exception, they have no lawful use in the United States. Jammers are not only designed to impede authorized communications and thereby interfere with the rights of legitimate spectrum users and the general public, they are also inherently unsafe. (Federal Communications Commission, 2012, para 2).

Jammers have the capability to interfere with critical public safety communications. As a result of these disruptions, emergency service professionals such as fire fighters and law enforcement officials are at a higher risk than usual. This increased risk also affects the public that emergency officials are responsible for helping. GPS jammers can also interfere with reliability of emergency calls and emergency transport navigations systems.

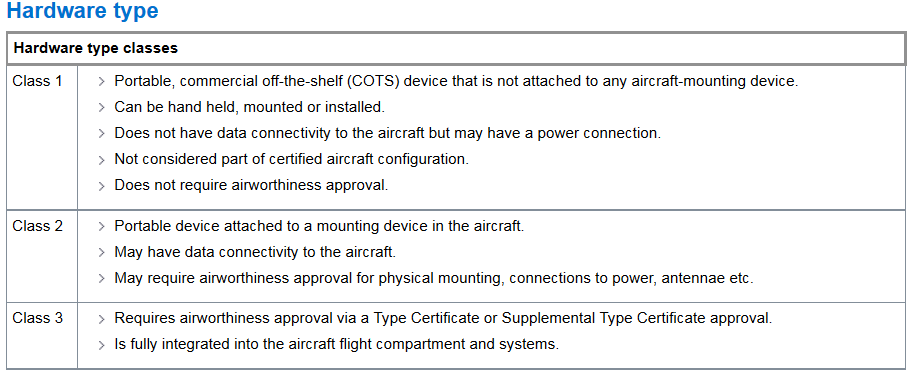
In order to protect the public and preserve unfettered access to emergency and other communications services, the Act and the Rules broadly prohibit the importation, use, marketing, manufacture, and sale of jammers. Consequently, the Commission has issued several enforcement advisories and consumer alerts emphasizing the importance of strict compliance in this area and encouraging public participation through the Commission’s jammer tip line. We expect individuals and businesses to take immediate steps to ensure compliance and to avoid any recurrence of this type of misconduct, including ceasing operation of any signal jamming devices that may be in their possession, custody, or control. We also strongly encourage all users of these devices to voluntarily relinquish them to Commission agents. (Federal Communications Commission, 2012, paragraph 2).

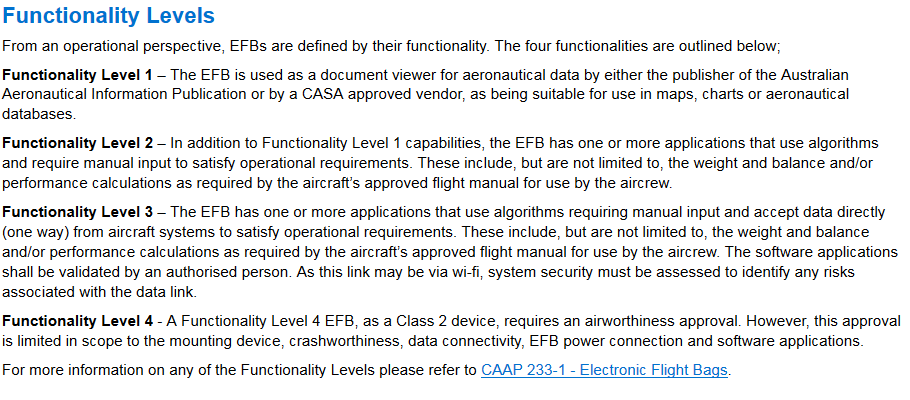
Bojczak's GPS jammer was using radio signals that range between the restricted frequencies of 1559 to 1610 MHz. This range is designated for the Radio navigation- Satellite service that is used for GPS to function. As a result of Bojczak interfering with sensitive aeronautical navigation equipment, he was fined $31,875 on the account that he voluntarily forfeited the GPS jammer device (Federal Communications Commission, 2012).

GPS jamming detection is not an easy task for law enforcement agencies. Previous investigations on this matter were not as successful. Between 2009 and 2011, the FCC and FAA were looking for another GPS jammer in a truck in the same area. It took two years to make an arrest for this specific jammer. A Google Internet search for GPS jammers will produce over a million results. It is not helpful that these devices are sold on the internet for as little as twenty five dollars (Brewin, 2013).

**EFB**

The EFB acts as an electronic display and storage system to rid the cockpit of conventional paper products. Documents found on a typical EFB include the Flight Crew Operations Manual, maps, charts, Minimum Equipment Lists and other flight operation files **(http://www.casa.gov.au/scripts/nc.dll?WCMS:STANDARD::pc=PC\_101196).** EFB allows automation of balance and weight tasks for the pilot. EFB's main function is to make pertinent documents more easily transported and accessible for the flight crew. There are different hardware types and levels of functionality of EFB. The following two figures give a more detailed description of both aspects **(Schonland, 2013).**





The threat involving EFB is that the data on the device can be lost or stolen in a few different ways. The physical device could be accidentally left somewhere or purposely stolen and the software could be compromised if pilots are not careful about downloading email attachments or using the internet. Taken from a study conducted by the aviation consulting company, AvIntel, it is reported that more than eighty percent of airlines that were surveyed utilize EFB, while forty percent of these airlines do not have an EFB cybersecurity plan in place (Schonland, 2013).

EFB has a big part in the cybersecurity framework that should be considered when protecting an aircraft. It is more of a risk that EFB data will be lost due to human error rather than failure of the EFB itself. Pilots who use public wireless Internet access for personal emails on their EFB devices are the currently the biggest threat. Some airlines that do not provide EFB's have created a bigger problem because the pilots are taking EFB into their own hands and using personal tablets to run these programs which may not be properly secured for such sensitive information (Schonland, 2013).

**Industry Response**

**FAA**

The FAA performed several studies on ADS-B and the strength of its security. These studies tested the system for collecting, storing and transmitting data. The FAA also performed risk assessments on the broadcast messages that ADS-B has been discredited for. ADS-B has passed all accreditation and certification adhering to the National Institutes of Standards and Technology (NIST) Information Technology (IT) standards. The FAA notes that this is an ongoing process to protect the availability confidentiality and integrity of ADS-B data.

Security Certification and Accreditation Procedures (SCAP) were implemented by the FAA to mirror Federal law requirements. ADS-B systems were tested under SCAP for the first time in 2008 and again in 2009.

This process ensures that ADS-B does not introduce new security weaknesses. It also ensures that the hardware and software composing the ADS-B systems meets rigid and well-documented standards for infrastructure security. ADS- B meets all qualifications and mandates of this process. As part of the SCAP, the system is tested annually for security compliance, and every 3 years the system goes through an entirely new SCAP. In addition, the FAA specifically assessed the vulnerability risk of ADS-B broadcast messages being used to target air carrier aircraft. This assessment contains Sensitive Security Information that is controlled under 49 CFR parts 1 and 1520, and its content is otherwise protected from public disclosure. While the agency cannot comment on the data in this study, it can confirm, for the purpose of responding to the comments in this rulemaking proceeding, that using ADS-B data does not subject an aircraft to any increased risk compared to the risk that is experienced today. (NEED HELP CITING THIS DOC, V. Security, Paragraph 5) http://www.gpo.gov/fdsys/pkg/FR-2010-05-28/html/2010-12645.htm

The FAA sent the research and analysis to other critical sectors of U.S. national infrastructure including the Transportation Security Agency (TSA), Department of Defense (DOD), the Secret Service and the Federal Bureau of Investigation (FBI). All agencies evaluated the methods that the FAA used to reach their conclusions, the risk assessment model used, and the projected outcomes. None of the agencies presented data against the original results of the FAA, that ADS-B does not bring higher risk to cyber threats to aircraft ( http://www.gpo.gov/fdsys/pkg/FR-2010-05-28/html/2010-12645.htm).

Upon risk assessment, the FAA states that the probability of malicious jamming or spoofing is slight. ADS-B systems do not make an aircraft any more vulnerable to attack than with previous SSR transmissions. Although alternatives were researched, the FAA found no reason to make a change in the transition to full use of ADS-B. The FAA will continue to collaborate with DHS and DOD officials in order to keep up with federal standards and threats to national security( http://www.gpo.gov/fdsys/pkg/FR-2010-05-28/html/2010-12645.htm).

On the contrary, there are FAA affiliated officials who share the same concerns as Teso, Haines, Costin and Argilo. Republican Congressman, John Mica oversees the FAA and is Chairman of the House of Transportation Committee. Mica specifically handles the implementation of NextGen and openly spoke to NBC News in 2012. He evaluated the progress made on NextGen in regard to information security flaws and rated it a D minus **(Stock, 2012).**

The FAA refused to speak directly to NBC News, however, a spokesperson came forward with a statement claiming that the FAA has been thoroughly investigating the potential security flaws. The spokesman, Ian Gregor, stressed that the FAA operates under strict continual validation and assessments of aircraft systems and the foundation of air traffic systems relies on their redundant testing for safety and assurance. Gregor stated that the FAA planned to maintain around half of its secondary radar systems as backup in the event of ADS-B failure. It is noted that the FAA considers this specific circumstance very unlikely **(Stock, 2012).**

**Boeing**

In 2012, Boeing requested to change onboard network systems on their Model 777-200, -300, and -300ER Series aircraft. This request was due to concerns about interconnectivity. These specific Boeing models were not built with the intention of indirectly connecting systems that perform vital functions to something like in-flight entertainment. Boeing requested this change to mitigate the security threats, whether malicious or unintended, that could compromise maintenance and safety of an aircraft. It is noted by Boeing that "regulations and current system safety assessment policy and techniques do not address potential security vulnerabilities, which could be caused by unauthorized access to aircraft data buses and servers" (https://www.federalregister.gov/articles/2013/11/18/2013-27343/special-conditions-boeing-model-777-200--300-and--300er-series-airplanes-aircraft-electronic-system)

**FCC**

The FCC spent many years working towards finding a solution to the illegal use of GPS jammers in the US. After an undercover investigation, in June 2014, the FCC served a Chinese GPS jammer vendor with the largest fine in FCC history, totaling $34.9 million. The company, named CTS. Technology Ltd, has been in the US market for jammer sales since 2012. CTS sold ten devices to undercover agents associated with the FCC. The agents were able to test the effectiveness of the units, reporting that they were capable of completely blocking cell phones and Bluetooth, GPS, satellite and Wi-Fi signals within a half mile. They were illegally advertising under false pretenses and selling these jammers on the Internet. The FCC is stopping the problem at the source, however, it is reported that in an undercover study, every third truck passing Portland International Airport in Oregon was using a jammer (Brewin, 2014; http://www.techtimes.com/articles/8888/20140622/fcc-fines-chinese-gps-signal-jammer-vendor-34-9-million.htm).

**Discussion of the Findings**

* highlighted portion of pg 30 in airport review mag. use as intro to findings and why it is so important to create standards \* huge target. 8 pages minimum

Polstra- more likely to cause disturbances and not possible to fully hijack a plane.

* See the PDF document under Week 7-8 of 695
  + This document will help you define 2nd level headers and themes for organizing the data
* You are presenting a wrap up of the facts presented in the Literature Review

**Recommendations**

* *How can localized cyber disruptions affect civil aviations on a larger scale?*
* *automated passport control pg 35 airport review magazine*
* 8 pages minimum
* See the PDF document under Week 7-8 of 695

**Conclusion**

* 4 pages minimum
  + This section is optional, but I would recommend including it as a more concise closing of your paragraph.
* See the PDF document under Week 7-8 of 695

**References**

International Civil Aviation Organization. (2011, October 13). *ICAO promotes aviation safety by endorsing English language testing.* Retrieved from http://www.icao.int/Newsroom/News%20Doc/PIO.21.11.EN.pdf

International Civil Aviation Organization. (2012, November 19-30). *Cyber security for civil aviation*. Retrieved from http://www.icao.int/Meetings/anconf12/WorkingPapers/ANConfWP122.1.1.ENo nly.pdf

Iasiello, E. (2013, July-August). *Getting ahead of the threat*. Aerospace America. Retrieved from http://www.aerospaceamerica.org/Documents/AerospaceAmerica- PDFs-2013/July-August-2013/Viewpoint-Getting-Ahead-AA-Jul-Aug2013.pdf

Missing Malaysia plane MH370: What we know. (2014, September 8). *BBC News Asia*. Retrieved from http://www.bbc.com/news/world-asia-26503141

ADS-B and Next-Gen Avionics. (n.d.) *Trig Avionics*. Retrieved from http://www.trig- avionics.com/adsb.html

Stoen, H. (2000, September 4). *Understanding IFR, what it is, how to do it.* Stoenworks, Inc. Retrieved from http://stoenworks.com/Tutorials/IFR%20Introduction.html.

CDTI. (2009, August 18). Federal Aviation Administration. Retrieved from http://www.faa.gov/about/office\_org/headquarters\_offices/ang/

offices/tc/about/campus/faa\_host/tnes/ATCSurveillance/software/cdti2/

Stratus 2. (n.d.) ForeFlight. Retrieved from http://foreflight.com/stratus

ADS-B weather products: what you'll see in flight. (2013, October 15). iPad Pilot News. Retrieved from http://ipadpilotnews.com/2013/10/ads-b-weather-products-what- youll-see-in-flight/

What does an EFB do?. (n.d.). *Civil Aviation Safety Authority*. Retrieved October 5, 2014, from http://www.casa.gov.au/scripts/nc.dll?WCMS:STANDARD:: pc=PC\_101196

Schonland, A. (2013, April 8). Cyber-security and aviation. AirInsight. Retrieved from <http://airinsight.com/2013/04/08/cyber-security-and-aviation/#.VDGTumOO5OF>

Greenberg, A. (2014, August 9). DefCon: You cannot ‘cyberhijack’ an airplane, but you can create mischief. SC Magazine. Retrieved from <http://www.scmagazine.com/>

defcon-you-cannot-cyberhijack-an-airplane-but-you-can-createmischief/article/

365465/

Strohmeier, M., Lenders, V., Martinovic, I. (2014, April 15). On the security of the Automatic Dependent Surveillance-Broadcast Protocol. University of Oxford, United Kingdom. Retrieved from http://arxiv.org/pdf/1307.3664.pdf

**Appendix OR Appendices**

[OPTIONAL – Insert your appendices here. Either the word Appendix or Appendices is used in the header, depending on how many appendices are included. Pagination began on the Main Body Text page with Arabic numeral 1; pagination on this page continues sequentially using Arabic numerals.]

Appendix A – Title

[An appendix is used to provide additional information that would be either distracting for the reader or inappropriate if it were in the main body of the text. Common types of appendixes include but are not limited to a large table, a word list, the informed consent form, a mathematical proof, a computer program that is new or unique to the research referred to in the paper, verbatim instructions to participants, original scales or questionnaires, and raw data. An appendix should be used only if it helps the reader understand and or evaluate the paper. Each appendix is listed with an alpha subheading (e.g., Appendix A, Appendix B, Appendix C).]