Spring 2023

Enhancing Cyberspace Monitoring in the United States Aviation Industry: A Multi-Layered Approach for Addressing Emerging Threats

Matthew Janson
Embry-Riddle Aeronautical University, jansonm1@my.erau.edu

MCMP 690-691 Graduate Capstone Project

Enhancing Cyberspace Monitoring in the United States Aviation Industry: A Multi-Layered Approach for Addressing Emerging Threats

Matthew Janson

Embry-Riddle Aeronautical University

Submitted to the Worldwide Campus

in Partial Fulfillment of the Requirements of the Degree of

Master of Science in Cybersecurity Management and Policy

May 3rd, 2023

Table of Contents

Abstract

This research project examined the cyberspace domain in the United States (U.S.) aviation industry from many different angles. The research involved learning about the U.S. aviation cyberspace environment, the landscape of cyber threats, new technologies like 5G and smart airports, cybersecurity frameworks and best practices, and the use of aviation cyberspace monitoring capabilities. The research looked at how vulnerable the aviation industry is from cyber-attacks, analyzed the possible effects of cyber-attacks on the industry, and suggests ways to improve the industry's cybersecurity posture. The project's main goal was to protect against possible cyber-attacks and make sure that the aviation industry is safe and secure.

Keywords: airports, aircraft, aviation, cybersecurity, cyberspace monitoring, cyber threats

Statement of the Project

The research conducted used mixed method analysis using a combination of quantitative and qualitative methods to make sense of the data collected. The quantitative methods involved collecting and analyzing numerical data related to U.S aviation cyberspace environment. This included examining the types of cyber-attacks that have occurred, their frequency, the financial impact on the industry, and the measures that have been taken to mitigate cyber threats. The qualitative methods involved collecting and analyzing non-numerical data related to the experiences and perspectives within the U.S aviation cyberspace environment. This included understanding common challenges faced by the industry in detecting and responding to cyber-attacks or areas where the industry can improve its cyberspace monitoring and response activities.

The literature review identified the most relevant emerging cyber threats towards the aviation industry, understand cybersecurity frameworks and best practices, and to evaluate the limitations of existing cyberspace monitoring capabilities. A multi-layered approach is suggested as a result of this research to improve U.S. aviation cybersecurity. This approach involves the use of cyberspace monitoring capabilities, including new cyber threat detection capabilities, in addition to improved respond and recover cybersecurity measures. The effectiveness of the proposed approach is evaluated using real world use cases and comparing existing capabilities.

Finally, the research project provides recommendations for improving the cybersecurity posture of the U.S. aviation industry. It suggests the adoption of cyber threat frameworks and best practices, the use of new cyber threat detection tools that use AI and ML, and improving cybersecurity training and education for pilots and aircrew.

Executive Summary

The U.S. aviation cyberspace environment is an important part of the country's critical infrastructure. It helps the economy grow and keeps travelers safe. However, the nature of cyber threats is rapidly changing, and more sophisticated cyber-attacks are aimed at the aviation cyberspace environment. To protect this environment, it is important to set up effective cybersecurity measures like cyberspace monitoring and response capabilities.

This research paper looks at the major actors in the U.S. aviation industry and how important cyberspace monitoring is in their specific cyber risk environments. It discusses how information technology (IT) and operational technology (OT) are becoming more vulnerable as they work together. It also talks about how this convergence is increasing the cyber-attack surface and how improved cyberspace monitoring capabilities can be used to detect cyber threats and respond to them. And finally, the research paper provides recommendations and future research areas for U.S. aviation cybersecurity.

Program Learning Outcomes

The research paper fulfils the first training objective by bridging the themes of the Internet, Security and Governance to be studied. It highlights how the aviation cyberspace environment is a critical infrastructure that needs to be protected from sophisticated cyber threats. It also emphasizes the role of cyberspace monitoring in ensuring the safety of the aviation industry and the economy.

The study paper satisfies the second training objective of applying the elements of the roles and duties of cybersecurity management. It explores the specific cyber risk environments of the major actors in the U.S. aviation industry and how they can set up effective cybersecurity measures like cyberspace monitoring to mitigate potential cyber risks.

The third training objective of documenting the role planning has in cybersecurity is fulfilled by the research paper. It discusses how new cyber technologies have a positive and negative impact to the aviation ecosystem. Similarly, IT and OT convergence is playing a role in the need for new cyber threat detection technologies.

The research paper also demonstrates knowledge with research literature and analytical procedures, as well as independent study on one or more aspects of cybersecurity management and policy, which is the fourth training objective. The paper utilizes analytical techniques to explore the importance of improving the aviation industry's cybersecurity and reducing the risks of cyber-attacks. The paper also provides recommendations and future research areas for U.S. aviation cybersecurity, which highlights the importance of planning in mitigating cyber risks.

Methodology

The methodology for this research paper used mixed method analysis using a combination of quantitative and qualitative methods. The study began with a comprehensive literature review to explore the current state of cyber within the U.S. aviation industry, identify the most relevant emerging cyber threats towards the aviation industry, understand cybersecurity frameworks and best practices, and evaluate the limitations of existing cyberspace monitoring capabilities. This review provided a comprehensive foundation for the research paper and helped establish a framework for evaluating the proposed multi-layered approach.

The proposed multi-layered approach involves the use of cyberspace monitoring capabilities including new cyber threat detection capabilities in addition to improved respond and recover cybersecurity measures. The effectiveness of the proposed approach was evaluated by using real-world use cases and comparing existing capabilities. Based on the study's findings, the research offers technical and non-technical recommendations for the U.S aviation industry and indicate areas for further investigation. The technical recommendations involve the use of new algorithmic techniques for cyberspace monitoring, while the non-technical recommendations focus on improving existing cybersecurity frameworks and cybersecurity training for pilots. The study's objectives were to offer important information that may be applied to enhance the cybersecurity posture of the U.S. aviation industry and to guide future studies in this area.

Introduction

Since its early beginnings, the transportation industry has been a catalyst for global change. The aviation industry has been a major driver in building the global economy we have today (Fox, 2016). During this major change, safety, security and governance were at the forefront, but the creation of cyberspace has brought the aviation industry to a turning technological point (Kölle et al., 2011). This type of digital transformation is a major factor in why the aviation industry is becoming dependent on cyberspace (Weinelt & Moavenzadeh, 2017).

The systems-of-systems (SOS) and associated cyber components that make up the aviation industry's cyberspace environment come from a variety of technological domains (Nobles, 2018). Cyber components include, but are not limited to, ground systems at airports, flight information systems, security screening, and many other technologies (Krause & Marinos, 2020). This situation has led to new attack vectors and targets, like cloud-based technologies and cyber-physical systems (Bocetta, 2022). These cyber-attack targets can cause major problems with flight operations, put the crew's and passengers' safety in danger, and hurt the industry's reputation (Bocetta, 2022). It is important for the aviation industry to take more proactive cybersecurity measures to lower the risk of cyber-attacks and protect against possible harm (Arampatzis, 2021).

World leaders are aware of the significance of aviation cybersecurity since cyber-attacks on one industry might have a domino effect on other industries, causing extensive disruption and financial harm (World Economic Forum, 2020). In order to help the U.S. aviation industry, this study's objective is to look at information concerning aviation cybersecurity and emphasize the

need for a more comprehensive, multi-layered approach. The results of this research will have important implications for improving the aviation industry's cybersecurity and lowering the risk of cyber-attacks. This research answered the following question: How can the U.S. aviation industry enhance its cyberspace monitoring and response capabilities to address emerging threats?

The Global Aviation Cyberspace Landscape

Throughout the past decade, the aviation industry has dealt with a number of cybersecurity issues that put safety and security at risk (Ukwandu et al., 2022). In 2015, a security researcher named Chris Roberts was able to change the flight controls on a United Airlines plane (Zetter, 2015). This led cybersecurity researchers (Thames, 2015) to ask, “Did the aviation industry fail cybersecurity 101?” The researchers noted that it was taking the aviation industry a long time to adopt cybersecurity measures, which made it a more likely target for cyber threat actors (Ukwandu et al., 2022). This trend continues to this day, and cyber threat actors are attacking aviation organizations. These cyber-attacks have led to large-scale data breaches, the theft of sensitive information, and problems with flight operations (Ukwandu et al., 2022).

Unfortunately, aviation cyber risks continue to get worse (Arampatzis, 2020). Several reports from the World Economic Forum, the U.S. Government Accountability Office, the International Air Transport Association, and the Atlantic Council show that the aviation industry is having trouble protecting its cyberspace environment (Arampatzis, 2020). The number of cyber-attacks on the aviation industry has significantly increased after the COVID-19 epidemic

(Arampatzis, 2021). Most of the time, this is due to bad cybersecurity practices, human error, a lack of money for cybersecurity, remote access, and cloud-based services (Arampatzis, 2021). According to a recent aviation cybersecurity report, the biggest global cyber-attacks were related to fake websites, data theft, phishing, and ransomware (Bocetta, 2022). These cyber-attacks can be stopped, but the aviation industry is still struggling to learn from past mistakes and meet basic cybersecurity measures while adopting new methods (Flessas, 2022).

The U.S. Aviation Cyberspace Environment

A large percentage of the American economy is the aviation sector (Brannon, 2020). More than 10 million American jobs and over $1.7 trillion in economic activity have been created by this sector (Brannon, 2020). This rise in social and economic activity is a direct cause of the growth of the cyberspace environment (Schaufele, 2020). As a result, the U.S. has been forced to resolve long standing cybersecurity issues like internet-accessible cyber systems, inadequate cybersecurity governance, surges in cyber vulnerabilities, and evolving cyber threats (Arampatzis, 2021).

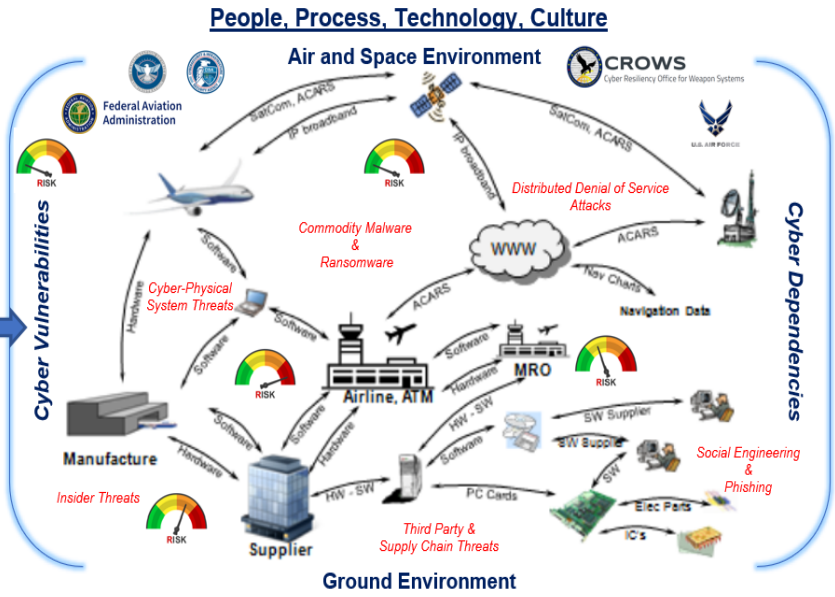
In the past, it was hard for cyber threat actors to target the aviation industry because it took a lot of knowledge to take advantage of its once disconnected and legacy technologies (Behler, 2015). As the U.S. aviation industry has become more software-driven, digital technologies have brought about big changes that affect how the industry operates (Behler, 2015). For the purpose of this paper, there are five cyberspace risk environments that make up the U.S. aviation cyberspace environment (Behler, 2015). They include airports, airline companies, aircraft support, aviation management, and aircraft systems (Behler, 2015). Together,

they make up the entire cyberspace environment and have their own organizations, processes, technologies, and cultures (Mahn et al., 2022). Figure 1 shows the different aviation organizations, core functions, shared cyber dependency, and possible cyber threats that make up this environment (Mahn et al., 2022).

Figure 1

The U.S. Aviation Cyberspace Environment

Cyber Risk Environment	Core Functions
Airport	• Day-to-Day Management • Food and Shopping • Information Management
Airline Company	• Ticketing and Passenger Loading • Customer Service • Flight Management (Carrier)
Aviation Management	• Airflow Management • Air Navigation Services • Collision Prevention
Aircraft Support	• Ground Support Functions • Ground Transportation • Ground Safety
Aircraft Systems	• Aircraft Operations • Aircrew Command and Control • Passenger Support



Note. The U.S. aviation cyberspace environment. Adapted from *A Framework for Aviation Cybersecurity*, American Institute of Aeronautics and Astronautics, (http://www.aiaa.org/aviationcybersecurity). Copyright 2013 by the American Institute of Aeronautics and Astronautics. Adapted with permission.

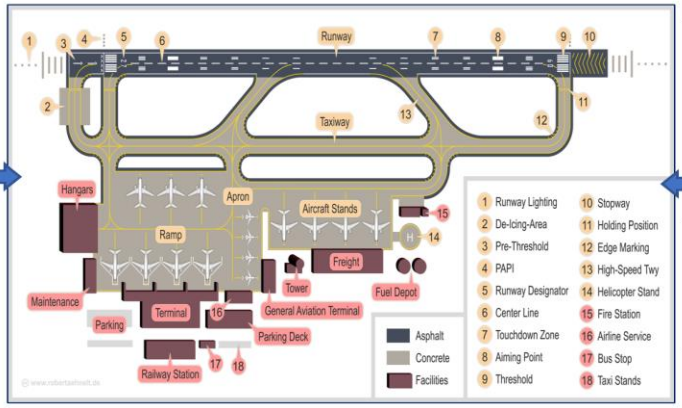
Cybersecurity for Airports and Airline Companies

Cyber-attacks can have a detrimental impact on airports due to the presence of financially motivated organizations such as retailers, restaurants, and airline companies (Nobles, 2018). These organizations are responsible for providing essential services to passengers and generating significant revenue for the airport (Nobles, 2018). Therefore, a cyber-attack that disrupts the operations of these organizations can lead to financial losses and damage to the airport's reputation (Nobles, 2018). Airports must deploy effective cybersecurity measures to stop and lessen the effects of cyberattacks and safeguard their vital assets and operations (Nobles, 2018). Figure 2 shows a notional airport ecosystem made up of cyber systems that work together to give passengers and airport staff a safe, secure, and customizable experience (Monteagudo, 2022).

Figure 2

The Airport Cyber Ecosystem

Airport System Category	Cyber Systems
Internal	LAN, VPN, IT equipment, Mobile network and apps, passenger WIFI, SOC, Flight Display Systems, etc.
External	GPS, cloud-based data, Network Security Management, WAN, Air to satellite communication systems, GIS, etc.
Airline/ Airside Operations	Air traffic management, flight tracking systems, departure control systems, airfield lighting and runway control and monitoring, cargo processing, aircraft re-fueling, etc.
Landside Operations	Landside operations systems control center, fuel management, lighting detection systems, parking management systems, etc.
Safety and Security	Access control systems, authentication systems, baggage screening and handling systems, surveillance systems, passenger screening, perimeter intrusion detection, emergency response, firefighting, etc.



Airport System Category	Cyber Systems
Customer Service	Cashpoint terminals, mobile payments, point of sales (PoS), duty free, catering, etc.
Facilities and Maintenance	Airport vehicle maintenance, building management and control systems, energy management systems, lifts and escalators, SCADA (utilities, roads, ancillary areas), environmental management systems, etc.
Passenger Management Systems	Kiosk devices, e-ticketing, electronic visual information display systems, passenger check-in and boarding, central reservation systems, etc.
Staff Management	Staff records management, authentication systems, mobility-enabled applications.

Note. The U.S. aviation cyberspace environment. Adapted from *A diagram showing the infrastructure of an airport*, by Robert Aehnelt, (https://en.wikipedia.org/wiki/Airport#/media/File:Airport_infrastructure.png). Copyright 2011 by ShareAlike 3.0 Unported. Adapted with permission.

This type of individual passenger experience is made possible in part by the use of mobile and wireless technology (Nobles, 2018). According to a survey by Inmarsat Aviation (2017), "60% of passengers expect to be able to use the internet at the airport and on their flight" (p. 3). This increased connectivity allows passengers to stay connected with friends and family, work remotely, or simply browse the internet while waiting for their flights (Inmarsat, 2017).

After an uptick in wireless cyber-attacks, several U.S. airports were involved in a nation-wide cybersecurity assessment, and the results were not pretty (Rayome et al., 2018). The cybersecurity assessment showed that several U.S. airports had poor wireless cybersecurity practices like the use of old technology, bad encryption, poor password management, and rogue access points (Rayome et al., 2018). The top offenders were airports in San Diego, Houston, Ft. Meyers, Dallas, Detroit, and Boston, to name a few (Rayome et al., 2018). Even with these types of cyber-attacks on the rise, the use of wireless systems continues to grow (Iyengar, 2022). A 2022 market study states that the U.S. aviation wireless market is valued at $1.5 billion (Global Industry Analysts, 2022).

New wireless technology like 5G is laying the groundwork for "smarter" airports. In a recent market study, Verizon (2021) talks about five ways that 5G technology will improve the aviation industry. The study states that 5G can provide faster internet connectivity, real-time data to find the best routes, augmented reality and virtual reality experiences, airport operations, and

improved in-flight entertainment and communication systems. These improvements require the use of more digital technology, but it comes with safety and cybersecurity concerns (Mariani et al., 2019). Recently, the Federal Aviation Administration (FAA) expressed concern about the risks that 5G technology poses for the aviation safety, especially for radio altimeters, which are important for landing planes (Shepardson, 2022). As a result, telecommunication companies are working with aviation organizations to fix these issues and embrace 5G technology (Shepardson, 2022). This situation shows the advantages and disadvantages of new technology, which need to be need carefully thought out and regulated (Shepardson, 2022).

Wireless technology is just one of many cybersecurity concerns with smart airports (Koroniotis et al., 2020). Smart airports often use legacy systems that are vulnerable to cyber-attacks, making it important for airports to regularly assess and upgrade their cybersecurity measures (Koroniotis et al., 2020). Newer systems are also making the attack surface grows, making it easier for cyber threat actors to break the security of the whole system (Koroniotis et al., 2020). The reliance on both legacy and new systems may create single points of failure that could disrupt airport operations (Koroniotis et al., 2020).

U.S. airline companies such as American, Delta, United, and Southwest are also primary customers of airport facilities and services (Tunčikienė & Katinas, 2020). These companies rely on airports to provide the infrastructure, services, and support necessary for their operations (Tunčikienė & Katinas, 2020). Airports serve as the hub for these airline companies, providing them with access to runways, taxiways, gates, terminals, and other facilities necessary for their flight operations (Tunčikienė & Katinas, 2020).

A recent news article describes how Airline companies are taking steps to improve their cybersecurity posture (Barrett, 2022). The author mentions that American Airlines is taking proactive steps to enhance its airport and aircraft cybersecurity posture (Barrett, 2022). They have put in place a number of cybersecurity measures, such as regular penetration testing and vulnerability assessments, to find and fix any weaknesses in their systems (Barrett, 2022). They have also spent money on cybersecurity tools and technology to prevent cyber-attacks, while accounting for resiliency in their operations (Barrett, 2022).

In the upcoming years, the U.S. aviation industry is anticipated to increase significantly. According to a report by the FAA, the complete number of passengers traveling by air in the U.S. is expected to nearly double over the next two decades, reaching 1.3 billion passengers by 2039 (Dickson, 2020). With these figures, it should come as no surprise that by 2030, investments in cybersecurity are anticipated to expand at the quickest rate in airports and airline industries (Daivanayagam, 2021). It is up to these aviation organizations to secure networks, systems, and data like sensitive passenger information, financial information, and flight plans (Mahn et al., 2022). Since these organizations rely on each other, cybersecurity responsibilities should be clear, linked to business practices, and made official across the airport ecosystem (Mahn et al., 2022).

Cybersecurity for Aviation Management

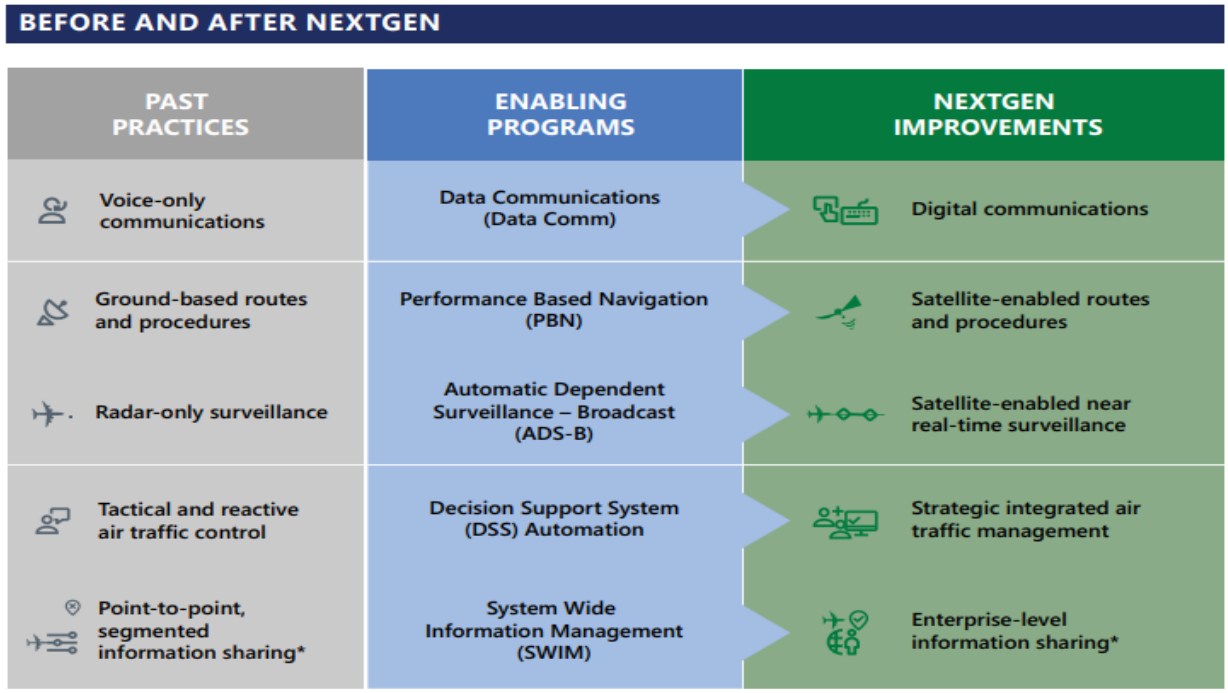
Aviation management organizations are a key part of making the U.S. aviation industry more secure (Wolfe, 2020). They do this by making and enforcing rules and regulations (Wolfe, 2020). The FAA, a U.S Department of Transportation Agency, is in charge of regulating and

supervising domestic civil aviation (Wolfe, 2020). The FAA oversees creating and implementing rules and standards for the design and maintenance of aircraft, issuing licenses to pilots and aircraft mechanics, and running the National Aerospace System (NAS) (Dickson, 2020).

The NAS is a complex SOS environment that integrates various cyber components, including air traffic control facilities, navigation aids, and communication systems (Dickson, 2020). The NAS relies on a robust set of cyber programs, which form the basis for managing air traffic, planning flights, and talking between air traffic controllers and pilots (Dickson, 2020). Figure 3 shows how the NAS is changing with the use of new cyberspace programs (Dickson, 2020).

Figure 3

The NAS Next Gen Transformation



Note. The Next Generation National Aerospace System. From *A Report on the History, Current Status, and Future of National Airspace System Modernization*, by Steve Dickson, (https://www.faa.gov/sites/faa.gov/files/2022-06/NextGenAnnualReport-FiscalYear2020.pdf). Copyright 2020 by The Federal Aviation Administration. Reprinted with permission.

After multiple investigations, the FAA is realizing how important cybersecurity is to the NAS and is taking steps to make its systems safer against cyber-attacks (Holemans, 2022). In 2015, the FAA began making changes to its cybersecurity program, like establishing cybersecurity roles and responsibilities, and supporting policies that make cybersecurity a permanent part of their business processes (Holemans, 2022). A key role in the cybersecurity program is the Cybersecurity Steering Committee, which oversees all parts of the FAA's cybersecurity mission (Grossman, 2021).

This decision-making element is forcing the FAA to integrate cybersecurity into their resource decisions. Recently, the FAA (2022) said “that airport terminal grants won't be given out unless efforts are made to consider and address physical and cybersecurity risks relevant to the transportation mode, type, and scale of the project.” This is a positive step to hold stakeholders accountable and make cybersecurity a top priority (Holemans, 2022).

Similar to the FAA, the Department of Defense (DoD) was met with the same scrutiny when it came to improving cybersecurity for weapon systems like aircraft (Chaplain, 2018). The U.S. Air Force (USAF) is taking a more proactive and cyber-resilient approach to cybersecurity (Welch, 2017). In 2017, the Cyber Resiliency Office for Weapon Systems (CROWS) became an official part of the USAF (Welch, 2017). The CROWS works to find and stop possible cyber

threats to weapon systems. It also makes sure that the systems are built and kept in a way that makes them resistant to hacking and other forms of cyber-attack (Welch, 2017).

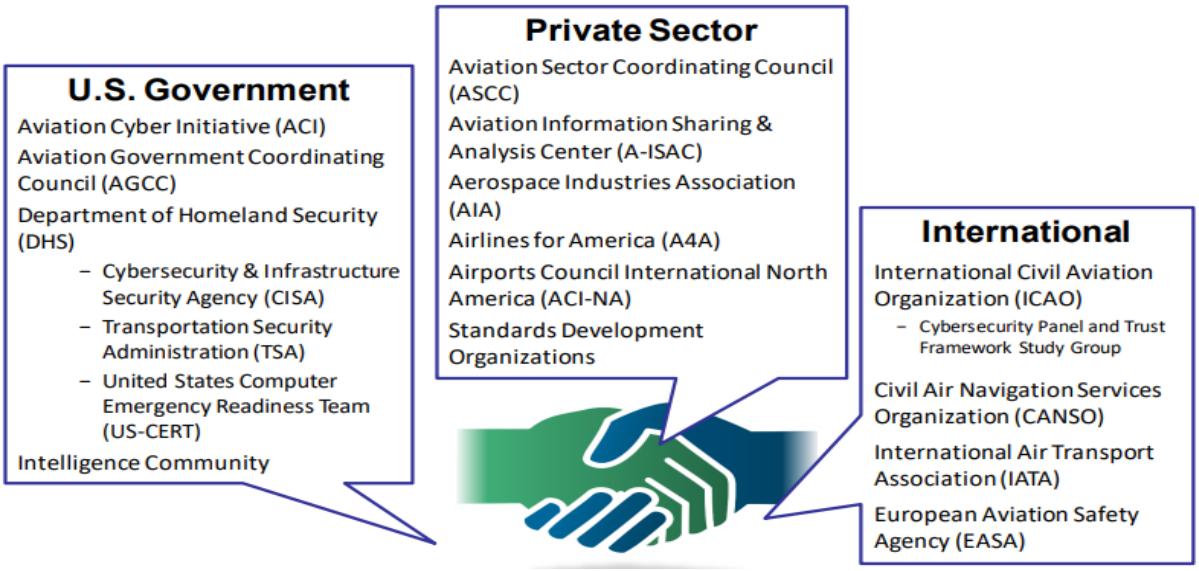
Even today, the FAA is looking into a number of ways to stay ahead of a technological change so they can respond more quickly to new cyber threats (Reed, 2022). A recent executive order is forcing the FAA to shift to using industry best practices like establishing a zero-trust architecture and micro-segmentation of different parts of networks (Reed, 2022). The key concept is to focus on securing the data of a specific application or service while presuming that networks have been compromised (McCollum, 2020). The Transportation Security Agency and the Cybersecurity and Infrastructure Security Agency (CISA), among others, are being compelled by this executive order to collaborate more closely with the FAA to create new cybersecurity guidelines and directions (Montgomery & Ma, 2022).

Aviation Cybersecurity Partnerships

These new relationships are giving rise to a "whole of government" task force called the U.S. Aviation Cyber Initiative (ACI) (Hampton, 2020). The FAA, the Department of Homeland Security, and the DoD are the primary organizations participating in this initiative (Hampton, 2020). The goal of the ACI is to make the NAS safer and protect the aviation industry's most important infrastructure from cyber-attacks (Hampton, 2020). Figure 4 shows how the ACI involves the collaboration of multiple government agencies to address cyber-attacks on the aviation industry (Hampton, 2020).

Figure 4

Aviation Cyber Initiative Stakeholders



Note. The U.S. Aviation Cyber Partnerships. From *Federal Aviation Administration ATO Cybersecurity Working Group Briefing*, Luci Holemans, (https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cas/acg/acg1.pdf). Copyright 2020 by The Federal Aviation Administration. Reprinted with permission.

The ACI includes several activities that are meant to find and fix weaknesses in the aviation industry (Hampton, 2020). These activities include new aviation cybersecurity research, performing regular cybersecurity assessments, and practicing cyber incident response using cyber table top exercises (Hampton, 2020). For example, the National Federation of Aviation Cyber Test Organizations and Researchers (N-FACTOR) is a key element of the ACI. The N-FACTOR supports the aviation industry with research, development, testing, and evaluation events (Hampton, 2020). The ACI also gives aviation organizations a way to share information and best practices, which helps to make the U.S. aviation industry safer as a whole (Hampton, 2020).

Another way to share cyber-relevant information and best practices is through the Aviation Information Sharing and Analysis Center (A-ISAC) (Francy, 2015). In 2014, the A-ISAC was formed by an international community of airports, airline companies, satellite manufacturers, aviation services, and supply chain companies (Francy, 2015). This community depends on the A-ISAC to give them accurate and up-to-date information about cyber threats and weaknesses that could affect their operations (Francy, 2015). These new relationships and approaches show the importance of working together and set a higher standard for the aviation cyber environment (Mayorkas, 2022).

Cybersecurity for Passengers and Investors

Aviation cybersecurity issues also affect passengers and investors (Ukwandu et al., 2022). Cybersecurity breaches can result in the loss of personal and financial information, which can harm customer trust and affect the financial performance of companies in the industry (Phillips, 2022). Most cybersecurity experts agree that about 20% of passengers face cyber threats when they travel (Tiwari, 2022). Cybersecurity for passengers should be very similar to current airport security measures (Ukwandu et al., 2022).

Airport security measures are filled with checkpoints, sensors, and constant reminders that if you “See Something Suspicious, Say Something" (Department of Homeland Security, 2021). Reporting suspicious cyber activity like social engineering and phishing attempts are cyber-related examples to this physical security program (Ukwandu et al., 2022). Furthermore, security checkpoints that come along with signing into an account or logging into a website are a natural part of extending the passengers safety and security into the digital realm (Tiwari, 2022). Multi-factor authentication, encryption, and data integrity mechanisms are no longer optional

(Tiwari, 2022). Basic cyber hygiene and cybersecurity awareness are part of an overall cultural shift that needs to occur for passengers (National Cybersecurity Alliance, 2022). U.S. agencies like CISA and the Federal Communications Commission have recently put out cybersecurity tips, under the "be cyber smart" motto, to make them less appealing targets (Federal Communications Commission, 2020).

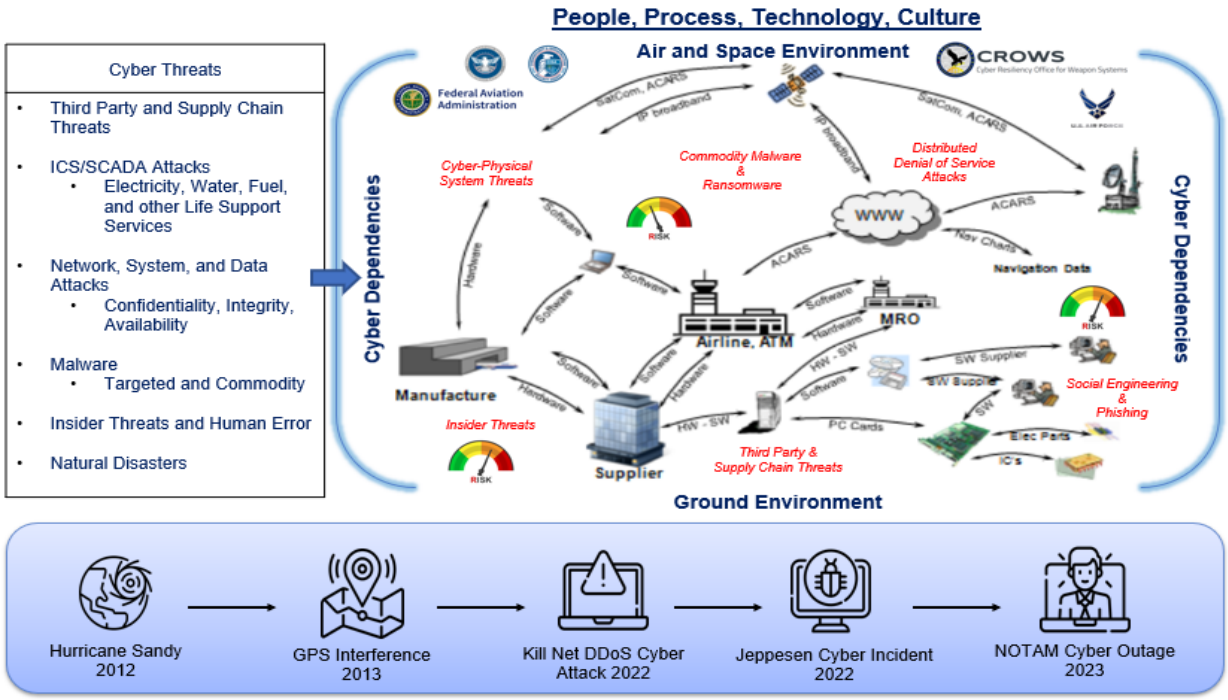
Cybersecurity is an important part of the aviation industry that affects everyone, from the companies that run the technology to the passengers who depend on the industry for travel and business (Watson, 2020). To handle aviation cyber threats and maintain the safety of air travel, a comprehensive strategy that considers people, procedures, technology, and culture is required (Mahn et al., 2022). Everyone in the industry needs to put cybersecurity at the top of their priority lost, especially as cyber threats evolve (Watson, 2020).

U.S. Aviation Cyber Threats Events

Cyber-attacks are becoming more prevalent in the U.S. aviation cyberspace environment, endangering the operations' confidentiality, integrity, and availability (Ukwandu et al., 2022). Cyber threat events can have minor consequences, such as a website going down, or more serious consequences, such as flights being canceled, delayed, or even putting flight safety at risk (Watson, 2020). Figure 5 shows the different types of cyber threat that can affect the aviation industry with varying degrees of consequence.

Figure 5

Cyber Threats in the U.S. Aviation Industry



Note. The major U.S. aviation industry cyber threat events from 2012-2023. Adapted from *A Framework for Aviation Cybersecurity*, American Institute of Aeronautics and Astronautics, (http://www.aiaa.org/aviationcybersecurity). Copyright 2013 by the American Institute of Aeronautics and Astronautics. Adapted with permission.

When the U.S. National Strategy for Aviation Security came out in December 2018, it included a section on cybersecurity because the impacts of cyber threat events on the aviation system are becoming a bigger problem (Arampatzis, 2020). The strategy described the importance of both hardening the aviation cyber environment to make it more difficult for cyber-attacks to occur, while being ready to respond to an actual cyber-attack (Arampatzis, 2020). Unfortunately, cyber threats are continuing to evolve and which requires better cyber threat detection and response actions (Arampatzis, 2020).

Intentional Cyber Threats

Sophisticated cyber threats are advanced and complicated, which makes them hard to detect (Alexandrovich, 2019). These threats often use cutting-edge tools and tactics, techniques, and procedures (TTPs) that are designed to get around traditional cybersecurity measures and avoid being found (Alexandrovich, 2019). Sophisticated cyber-attacks are planned and carried out by skilled and determined attackers who have a clear goal in mind (Alexandrovich, 2019). These attackers may use ransomware, malware, phishing, and denial-of-service (DoS) attacks to wreak havoc on the aviation industry (Alexandrovich, 2019).

In October 2022, a group of pro-Russia hackers called "Killnet" orchestrated a coordinated DoS attack that made the websites of several major U.S. airports inaccessible (Wallace et al., 2022). The cyber-attack, which involved sending a lot of useless data to the targets, broke the airport's public-facing websites at Hartsfield-Jackson International Airport in Atlanta, Los Angeles International Airport, Orlando International Airport, and Chicago's O'Hare and Midway International Airports (Wallace et al., 2022). A month later, there was an even more consequential cyber-attack.

On November 2, Jeppesen, which is a part of Boeing, said on its website that some of its products and services had been affected by a "cyber incident (Godlewski, 2022)." This implied that navigational charts and other data that the majority of pilots obtain from their electronic flight packs might not function properly (Godlewski, 2022). It was discovered soon after the event that Jeppesen was not the intended target of the attack, but that the information distribution system itself was flawed (Godlewski, 2022). The Jeppesen incident shows how vulnerable flight information systems are and how much they impact day-to-day operations (Bocetta, 2022). The

incident gave thousands of pilots a real-life lesson because it made it hard for them to download the most recent navigation, flight planning, and instrument approach data (Janofsky, 2022). This lesson was a good reminder that the aviation industry depends on cyberspace and the need for accessible backup tools is a necessity (Myers, 2022). These aren't the only major cyber threat events in the past few years.

There are several documented cases of ransomware and phishing cyber-attacks (Bocetta, 2022). In 2021, two U.S. aviation organizations, VT San Antonio Aerospace and Spirit Airlines, fell victim to separate cyber-attacks (Ahmed, 2020). A ransomware attack on VT San Antonio Aerospace, a company that fixes planes, led to the theft of confidential information about the company's employees and clients (Ahmed, 2020). In exchange for the safe return of the stolen data, which included employee names, social security numbers, and customer contact information, the attackers demanded a ransom (Ahmed, 2020). Following that, the stolen data was offered for sale on the shadow web (Ahmed, 2020).

In parallel, Spirit Airlines, a Florida-based airline company, was hit by a ransomware attack (Kostka, 2022). The hackers were able to get sensitive information like customer names, addresses, dates of birth, and passport information from the airline's systems (Kostka, 2022). Although the airline company has not disclosed whether it paid the ransom, the hackers posted some of the stolen data on the dark web as proof of the breach (Kostka, 2022). These events show how serious cyber threats are and how they can affect the aviation industry (Kostka, 2022).

Ransomware attacks are a growing threat to aviation organizations, with the potential to cause severe disruptions and significant financial losses (Bocetta, 2022). Cybersecurity Ventures (2021) says "that the damage caused by ransomware will cost the world $20 billion by 2021, up

from $11.5 billion in 2019." To protect against these kinds of attacks, aviation organizations need to stay alert and take the right steps to secure their networks and systems, such as making regular backups of important data, teaching employees about best practices for cybersecurity, and using multi-factor authentication for sensitive accounts (Humphries, 2021). Ransomware attacks have proven that losing important systems and data can have big effects on an organization's finances and reputation, and may even lead to bankruptcy (Bocetta, 2022).

Throughout the past two decades, most cyber-attacks on the aviation industry happened in North America, followed by Europe (Ukwandu et al., 2022). During this time, 2018 became a record setting year with the highest rate of cyber-attacks in U.S. history (Ukwandu et al., 2022). As a result, over 94 million people were affected and planes grounded for about five days straight (Ukwandu et al., 2022). Since then, cyber-attacks continue to increase for the aviation industry. A report from 2021, states that 52% of aviation organizations experienced a cyber-attack, airline companies being the primary target in 61% of the attacks, and that 34% of those attacks led to sensitive data being leaked (Bocetta, 2022).

Unintentional Cyber Threats

On the other hand, unintentional cyber threats are caused by humans or technical faults in the system (Watson, 2020). These include things like human-error, data leaks, misconfigurations, software bugs, and system failures (Watson, 2020). In 2013, a truck driver near Newark Liberty International Airport in New Jersey used a $100 Global Positioning System (GPS) jammer while driving close to the airport (Thomson, 2013). This caused interference with GPS signals that were being used in air traffic control systems (Thomson, 2013). Eventually, the Federal Bureau

of Investigation was forced to intervene, and the truck driver was fined over $40,000 (Thomson, 2013).

This incident shows how fragile the U.S. aviation industry is to GPS cyber threats (Thomson, 2013). Shortly after, the FAA asked the Radio Technical Commission for Aeronautics to look into how GPS interference might affect the pilot's ability to fly. The study showed how important it is for pilots to receive the proper training on how to recognize and deal with GPS interference and found several ways that training could be improved (Rexroth, 2018). Among these are better ways for pilots and air traffic controllers to talk to each other and more realistic training scenarios that show how interference affects flight instruments (Rexroth, 2018). Even with these recommendations, the FAA hasn't provided a meaningful policy or technical solution to address the problems that exist (Harris, 2022).

Another major concern is system outages caused by natural disasters (Bocetta, 2022). One of the largest outages to affect air travel happened in October 2012 when Hurricane Sandy struck the East Coast (Moore, 2012). The mega storm caused widespread power outages, flooding, and transportation disruptions (Moore, 2012). Over nine airports, like the John F. Kennedy International and LaGuardia airports in New York City, had to close temporarily because of the hurricane (Goodwyn, 2012). Aviation management was also affected by the storm, which caused many flights to be canceled or delayed (Goodwyn, 2012). This is just one example of how natural disasters can affect the U.S. aviation industry's ability to keep critical infrastructure up and running (Watson, 2020). In these situations, aviation organizations need to have strong plans for handling cyber incidents that are linked to their continuity of operations and disaster recovery plans (Watson, 2020).

Human error is also a serious issue because they are considered to be one of the weakest links in cybersecurity (J. Cano M., 2019). This happens when employees accidentally download malware, lose or share private information, or make unauthorized system changes (Behler, 2015). A recent study shows that 85% of data breaches were caused by humans, with 94% of malware delivered via email (Koziol & Bottorff, 2022). This is why basic cybersecurity training and hygiene practices are so important (Kotler, 2022).

Cybersecurity training makes people aware of the risks and threats that come with using technology, such as phishing scams, malware, and other types of cyber-attacks (Koziol & Bottorff, 2022). Cyber hygiene means using strong passwords, updating software, and avoiding attachments or links in e-mail that appear suspicious (Kotler, 2022). These cybersecurity practices help organizations and people take the right precautions and avoid doing things that could put them at risk of cyber threats (Kotler, 2022). However, even with training, humans make mistakes.

In January 2023, the FAA Notice to Air Mission (NOTAM) system went down because personnel failed to follow procedures, demonstrating the impact of human error on aviation systems (Moon, 2023). The NOTAM system enables pilots to monitor factors that may have an impact on flights, including runway construction, local weather, and other crucial information required to ensure passenger safety (Kumpf, 2023). The system outage caused thousands of flights to be delayed or canceled, while highlighting another example of how fragile the aviation cyberspace environment is (Muntean & Wallace, 2023).

The NOTAM event also highlighted another cybersecurity issue, technical debt (Edwards, 2021). Technical debt is the cost that comes from the trade-offs between delivering

cyber components quickly and the long-term cost of maintaining, updating, and supporting those cyber components in the future (Edwards, 2021). Technical debt can significantly affect the safety, security, and general effectiveness of the aviation sector (Edwards, 2021). One example of how technical debt can affect the aviation industry is in the case of legacy systems (Kumpf, 2023). Legacy cyber systems are still used by many airlines for important tasks like air traffic control, reservations, and maintenance (Kumpf, 2023). These cyber systems don't always get the security updates they need, which leaves them open to cyber-attacks (Kumpf, 2023).

Overall, cyber threats in the aviation industry pose a big risk to the safety, security, and economic stability of the industry (Watson, 2020). As the aviation industry depends more on cyberspace, it is becoming more vulnerable to cyber threats, both on purpose and by accident (Watson, 2020). These threats can have a big effect on the whole ecosystem, including airline companies, airports, air traffic control, and the safety of passengers and crew (Watson, 2020). To deal with these problems, the aviation industry needs to adopt strong cybersecurity frameworks and best practices that strike a balance between confidentiality, availability, integrity, and resilience (Watson, 2020).

Aviation Cybersecurity Standards, Frameworks, and Best Practices

Cybersecurity standards, frameworks, and best practices are essential for the U.S. aviation industry to regulate and maintain airworthiness (David, 2021). The International Air Transport Association keeps a list of cybersecurity frameworks, standards, and guidelines that apply to civil aviation (IATA, 2021). The evolution of cybersecurity requirements continues to this day (David, 2021). In the past few years, various governmental organizations and regulatory

bodies have come up with frameworks, standards, and guidelines to make sure that the aviation industry meets the necessary cybersecurity requirements (David, 2021).

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is an example of a U.S. voluntary framework that gives a complete and flexible set of rules for managing and reducing cybersecurity risk in critical infrastructure sectors like aviation (Barrett, 2020). In 2018, the Aerospace Industries Association published a complementary framework called the National Aerospace System 9933 Cyber Defense Framework that provides a way to measure cyber defense capability levels, which coincide with the NIST CSF functions (Biesecker, 2018). The FAA has also developed its own set of cybersecurity guidance for different parts of the aviation cyber risk environment (David, 2021).

The Airport Cooperative Research Program 140 Guidebook on Best Practices for Airport Cybersecurity gives a framework for dealing with cybersecurity risks and weaknesses that are unique to airports, such as the best ways to protect airport systems and data (David, 2021). The National Safe Skies Alliance Quick Guide for Airport Cybersecurity, on the other hand, is a condensed, easy-to-use guidebook that gives airports steps they can take to improve their cybersecurity (David, 2021). Both FAA resources are meant to help airports improve their cybersecurity and lower the risk of cyber-attacks (David, 2021).

The FAA has also set specific cybersecurity requirements for aircraft systems and networks to make sure that the U.S. aviation industry is safe, compliant, and able to fly (David, 2021). The DO-326A/ED-202A Airworthiness Security Process Specification is one of the most important rules (David, 2021). It gives advice on how to build a cybersecurity risk management process for aviation systems and spells out what needs to be done to reach a level of

cybersecurity that allows planes to fly safely (David, 2021). Organizations in the aviation industry have to follow DO-326A and ED-202A, and if they don't, the FAA can take action against them, such as fines and penalties (David, 2021). Unfortunately, a 2016 study shows that an average of 40% of U.S. aviation organizations do not follow DO-326A/ED-202A requirements (Rockwell Collins, 2016).

The EU General Data Protection Regulation (GDPR), which sets rules for how personal data can be collected and processed in the European Union (Sheble, 2020), has also had an effect on the aviation industry. Before collecting and using someone's personal information, companies must get their clear permission and make sure the information is handled in a safe and clear way, according to the regulation (Sheble, 2020). If aviation organizations don't follow GDPR, they could face heavy fines (Sheble, 2020). In light of this, many aviation organizations have put a lot of money into improving their data protection and privacy practices (Sheble, 2020). GDPR has also made airlines rethink how they collect data, and some companies have decided to limit the amount of personal information they get from passengers to make sure they don't break the law (Sheble, 2020).

The FAA is also working with the International Civil Aviation Organization (ICAO) to harmonize these security rules (Pecharromán, 2021). At the moment, ICAO uses the ISO/IEC 27001 cybersecurity framework as the main standard in the aviation industry (Pecharromán, 2021). ISO/IEC 27001 is an international standard that tells how to set up, implement, maintain, and improve information security management systems (Pecharromán, 2021). The U.S. aviation industry benefits from the fact that most NIST CSF functions and NIST 800-53 security controls map directly to ISO/IEC 27001 (Pecharromán, 2021).

Over the years, cybersecurity frameworks in the aviation industry have changed a lot (David, 2021). Different standards and best practices have been created and updated to deal with the growing threat of cyber-attacks (David, 2021). Standardization efforts are a natural part of securing the aviation cyberspace environment, but the industry is still having trouble making them official because they don't know where to start (David, 2021). Most of the time, the first step is to understand why cybersecurity is important to the organization and create cybersecurity program that includes cyberspace monitoring (David, 2021).

Aviation Cyberspace Monitoring

Cyberspace monitoring is an important aspect of a comprehensive cybersecurity program (Holden et al., 2018). It involves keeping an eye on the aviation cyber environment so that cyber threats can be found and dealt with in a timely manner (Holden et al., 2018). The four primary processes are monitoring for insider threats, finding and protecting against malware, conducting cybersecurity operations, and dealing with cyber incidents (Murphy et al., 2015).

Insider Threat Monitoring

Insider threats are a big risk to airport cybersecurity, so monitoring for these threats is an important part of continuous monitoring (Murphy et al., 2015). According to the Airport Cybersecurity Best Practices Guidebook, current or former workers, contractors, vendors, or other anyone with authorized access to airport systems can pose an insider threat (Murphy et al., 2015). Figure 7 shows that insider threats could lead to the loss of data, system downtime, or physical damage (Costa D., 2017).

Figure 7

An Overview on Insider Threats

Note. An Overview of the Insider Threat. From *The U.S. CERT Definition of Insider Threat*, Carnegie Mellon University Software Engineering Institute, (https://insights.sei.cmu.edu/media/images/it-def2.original.png). Copyright 2017 by Carnegie Mellon University Software Engineering Institute. Reprinted with permission.

In order to keep the airport safe from possible attacks, insider threat monitoring is a constant process that must be continually improved (Murphy et al., 2015). Continuous monitoring involves the regular assessment of insider threat monitoring controls, identifying areas for improvement, and making necessary changes (Murphy et al., 2015). This process

makes sure that the insider threat monitoring program is effective, up-to-date, and able to adapt to the constantly changing insider threat landscape (Murphy et al., 2015). Continuous monitoring of insider threat monitoring is critical for maintaining a robust insider threat monitoring program and ensuring airport operations are secure (Murphy et al., 2015).

Malware Detection and Protection

Malware is another major cyber threat to aviation cybersecurity (Murphy et al., 2015). Malware is a type of malicious software that can infect systems and cause harm to aviation organizations (Murphy et al., 2015). These organizations are at risk of malicious email, infected websites, or malicious software downloads (Murphy et al., 2015). The Maersk cyberattack demonstrated how malware may ground aircraft and ships (Shead, 2022). The cyber-attack was caused by a variant of the Petya ransomware and resulted in significant disruption to Maersk's operations, with the company estimating losses of up to $300 million (Greenberg, 2018).

According to Maersk, the cyber-attack began when the malware was spread via a phishing email that targeted employees in Ukraine, where Maersk has a significant presence (Greenberg, 2018). Once the malware infected a computer, it quickly spread across Maersk's global network, causing widespread damage and data loss (Greenberg, 2018). The Maersk cyber-attack serves as a cautionary tale for aviation organizations of all sizes about the importance of cybersecurity and the potential consequences of a malware (Greenberg, 2018). To lessen the danger of malware, it's crucial for aviation organizations to have a robust malware detection and protection program implemented. (Murphy et al., 2015).

Once thought to be a good way to protect against malware cyber-attacks, the "air gap" is now thought to be a myth (David, 2021). Keeping cyber-attacks from happening by physically

separating critical systems from the internet or other networks is no longer a sufficient way to protect against modern cyber threats (David, 2021). A recent study reveals a 15-year effort by nation-states to breach air-gapped networks (Dorais-Joncas & Muñoz, 2022). The researchers describe how cyber threat actors developed and used various TTPs to jump the air gap and steal data from sensitive networks (Dorais-Joncas & Muñoz, 2022).

The study talks about how the cyber threat actors used tools like custom malware, TTPs, USB devices, and external hard drives to get data out of systems with air gaps (Dorais-Joncas & Muñoz, 2022). The researchers discovered that the malware used by the threat actor was designed to avoid detection by using various obfuscation techniques, such as code signing certificates, and by bypassing traditional security measures (Dorais-Joncas & Muñoz, 2022). Additionally, it highlights the importance of keeping software up-to-date, regularly patching vulnerabilities, user education and training, and an adequate backup strategy to reduce the risk of malware-related cyber-attacks (Dorais-Joncas & Muñoz, 2022).

Adequate malware detection and prevention techniques must be used in order to establish a successful malware detection and protection program (Rohith & Kaur, 2021). Methods for detecting and preventing malware include signature-based, behavior-based, and heuristic-based detection techniques (Rohith & Kaur, 2021). By using recognized malware signatures, signature-based detection can detect malware (Rohith & Kaur, 2021). To assess whether software is acting maliciously, behavior-based detection analyzes the software's behavior (Rohith & Kaur, 2021). Heuristics-based detection includes examining the software's source code to see whether any malicious code is there (Rohith & Kaur, 2021). The overall goal of malware detection and

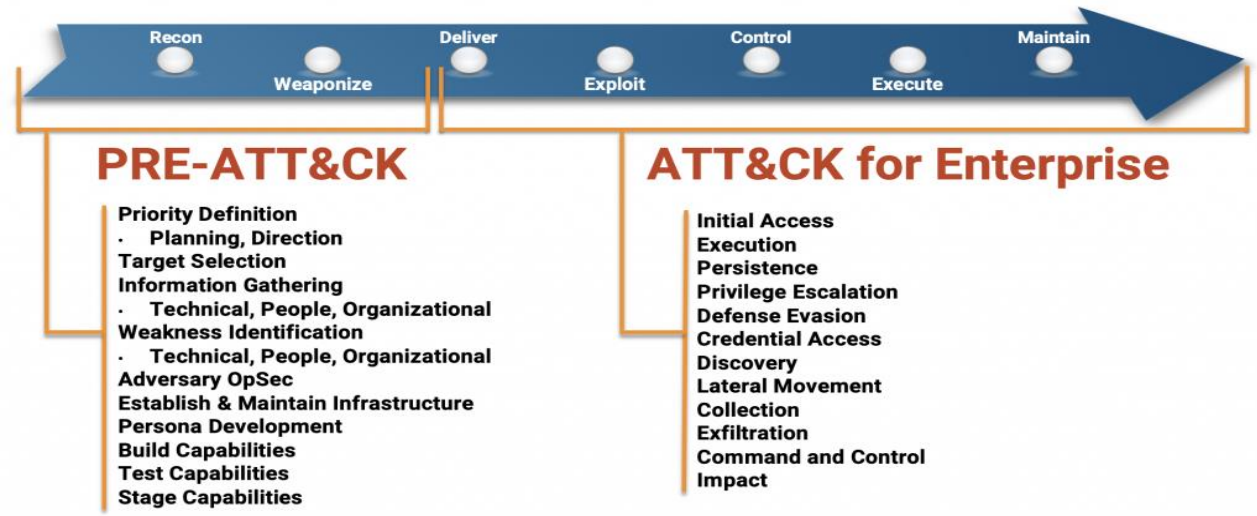
protection programs is to stop malware from getting into systems and lower the risk of data theft, data loss, and system disruption (Murphy et al., 2015).

Cybersecurity Operations

Cybersecurity operations are the centralized management and coordination of cyberspace monitoring and incident response activities (Kaliyaperumal, 2021). This includes collecting and analyzing data from different sources, like network traffic, system logs, and security alerts, to find possible security problems and decide how to handle them (Kaliyaperumal, 2021). SOCs frequently employ MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) Framework as their primary cyber threat framework (Strom et al., 2020). The framework can be used for adversary emulation, red teaming, behavioral analytics development, and maturity assessments (Strom et al., 2020). Figure 8 shows how MITRE ATT&CK is used in conjunction with the cyber-attack lifecycle to describe adversarial behavior using TTPs.

Figure 8

MITRE's Adversarial Tactics, Techniques, and Common Knowledge Framework



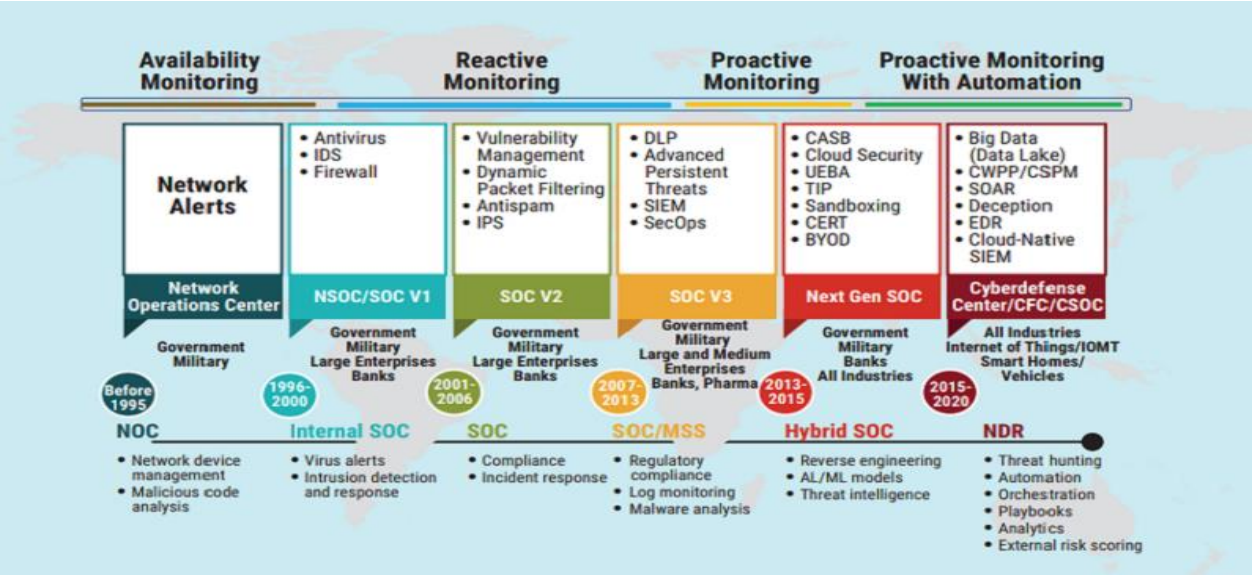
Note. The Cyber Attack Lifecycle and MITRE ATT&CK Framework.

From *MITRE ATT&CK: Design and philosophy* by MITRE, 2020, The MITRE Corporation, (https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy). Copyright 2020 by the MITRE Corporation. Reprinted with permission.

A recent study by MITRE (2022) says that one of the best ways to make a cybersecurity operations center is to take a proactive approach. The report provides eleven recommendations for creating and running a top-notch SOC to efficiently identify, stop, and deal with cyber-attacks (Knerler et al., 2022). Among the strategies are having a clear mission and vision, building a skilled and diverse team, doing proactive threat hunting, using automation and orchestration, making a strong security culture, and keeping up with new technologies and threat intelligence (Knerler et al., 2022). Figure 9 shows how SOCs have evolved to become more proactive and automated.

Figure 9

The Evolution of the SOC



Note. The global evolution of SOCs. From *The evolution of security operations and strategies for building an effective SOC,* Information Systems Audit and Control Association (https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc). Copyright 2021 by the Information Systems Audit and Control Association. Reprinted with permission.

The study also stresses the importance of continuous improvement through metrics and feedback, effective communication and collaboration between teams and stakeholders, and strategic partnerships with outside organizations (Knerler et al., 2022). Overall, the study gives organizations a full set of instructions on how to build and run a SOC that can protect them from cyber threats (Knerler et al., 2022).

The need for cybersecurity operations is causing aviation organizations to decide whether to keep SOC functions in-house or outsource them to a third-party organization (Miller et al., 2021). For example, Airbus and SITA recently joined forces to help the aviation industry with third-party SOC services (Lopamudra, 2017). These services rely on cyberspace monitoring capabilities like security information and event management systems and logging tools to find cyber threats (Krause & Marinos, 2020).

As "e-enabled" aircraft become more common, these SOC functions are starting to go beyond the typical airport cyberspace environment and include the actual aircraft system (Zmud et al., 2018). New guidance was recently published standardizing logging on e-enabled aircraft (IATA, 2021). The ARINC 852 guideline describes what security events should be logged, how long to keep logs, how to back them up, and how to encrypt them to keep the log data secure (IATA, 2021). By following the ARINC 852 guideline, SOC analysts can make sure they are

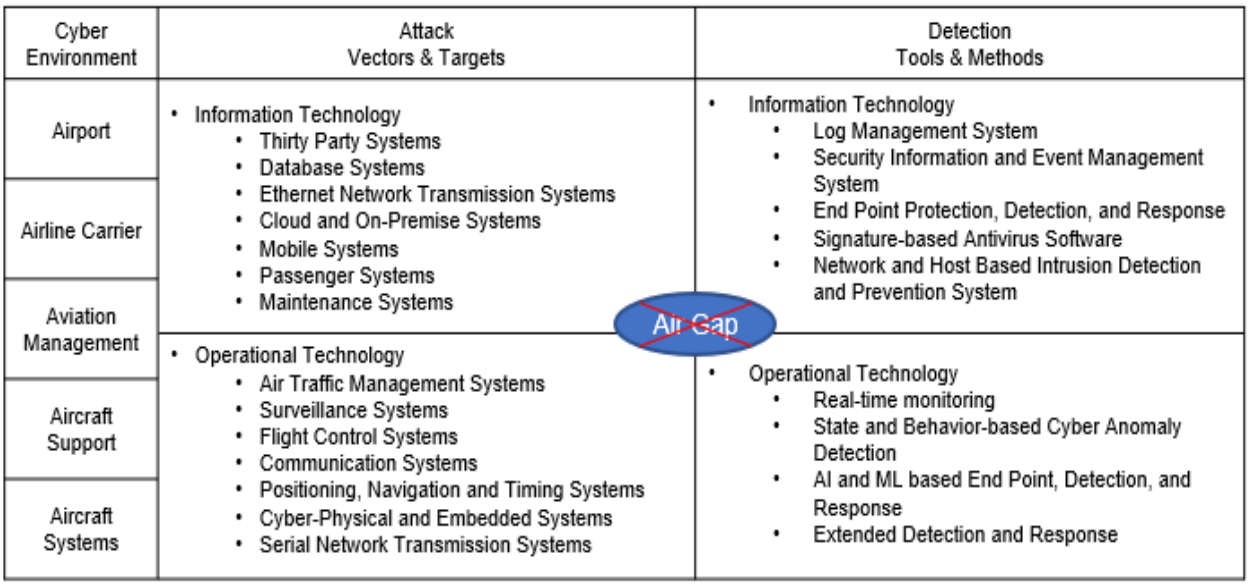
collecting and storing the right information to find and respond to possible security incidents (Krause & Marinos, 2020).

The fact that e-enabled aircraft is a combination of IT and OT is another reason why cyberspace monitoring needs to be improved (David, 2021). While this integration can offer many benefits, such as improved efficiency, it also creates new cyber-attack surfaces and makes it easier for cyber threat actors to cause harm (David, 2021). IT and OT convergence makes cyber-attacks easier because it lets cyber threat actors use the connectivity between systems that used to be separate (David, 2021). Once they get in, they might be able to move laterally through the converged network to get to their attack target. For example, if an aviation company's IT network is connected to its OT system, a cyber-attack on the IT network could also affect the OT system, which could lead to physical damage, production downtime, or even a safety incident (David, 2021).

This type of situation is described in a MITRE technical report. The authors propose a novel approach called Platform Independent Vectors of Techniques (PIVOT) for system-of-system attack path analysis (Zuniga & Janson, 2022). PIVOT can be used to describe ways an attacker could break into multiple systems that are part of a larger SOS environment, like aircraft systems (Zuniga & Janson, 2022). The authors say that PIVOT is a better way to analyze attack paths than traditional methods because it is more complete and can be used with existing cyber risk assessments (Zuniga & Janson, 2022). Figure 10 shows this IT and OT convergence in addition to the diminishing air gap.

Figure 10

IT/OT Convergence within the U.S. Aviation Cyberspace Environment



Aviation cyber components are no longer separate from the internet and other networks, which makes them more vulnerable to cyber-attacks (David, 2021). Attackers can use flaws in these aircraft systems to cause physical harm or stop critical functions from working while flying (David, 2021). Because of this, it's crucial to comprehend how crews and pilots would react to a cyber-attack (David, 2021).

A recent human-factors study looked at pilots' readiness for a cyber-attack (Gontar et al., 2018). The pilots were involved in two experiments: one with and one without training (Gontar et al., 2018). The results showed that pilots who had training were more likely to recognize cyber-attacks and respond to them than pilots who did not have training (Gontar et al., 2018). The research also showed how important it is to train pilots in cybersecurity so they can be prepared for possible cyber-attacks (Gontar et al., 2018).

Cyber-attacks are becoming a bigger problem in the U.S. aviation industry, which shows how important it is to have good cybersecurity operations (Cogburn, 2022). For critical infrastructure and sensitive data to be safe, there needs to be a well-designed security architecture as well as good communication and teamwork between different teams (Cogburn, 2022). By leveraging these resources, the U.S. aviation industry can keep up with emerging threats and protect against cyber-attacks (Cogburn, 2022).

Cyber Threat Detection Technology

Another way to keep up with emerging threats is to use new cyber threat detection technology (Cogburn, 2022). New intrusion detection and prevention systems are using artificial intelligence (AI) and machine learning (ML) methods to look at big data and find patterns that could point to a cybersecurity event (Mitchell & Chen, 2014). One of these methods is called "anomaly detection," and it is used to find strange or unexpected behavior on aircraft networks and systems, like strange patterns of access to a certain system (Mitchell & Chen, 2014). Behavior analysis is another way to find patterns that could be signs of bad behavior (Mitchell & Chen, 2014). This means using specialized algorithms to look at how users and systems act and figure out when a user is accessing data or systems (Mitchell & Chen, 2014).

New cyber threat detection technology has also been the subject of numerous research projects (Bellamy, 2019). A recent study gives a basic look at how different parts of intrusion detection systems (IDS) work in a commercial avionics system that uses the ARINC 429 communications bus (Ryon et al., 2020). The research not only gives the results of evaluating a

prototype avionics IDS, but it also takes into account important aspects of the avionics cyberspace environment (Ryon et al., 2020).

Another research study focused on an IDS solution for the MIL-STD-1553 communications bus. The proposed IDS was designed to detect anomalies in the communication bus traffic that may indicate a cyber-attack (Stan et al., 2020). These new IDS capabilities offer better coverage and techniques to discover cyber threats in the avionics cyberspace environment (Bellamy, 2019).

Cyber Incident Response

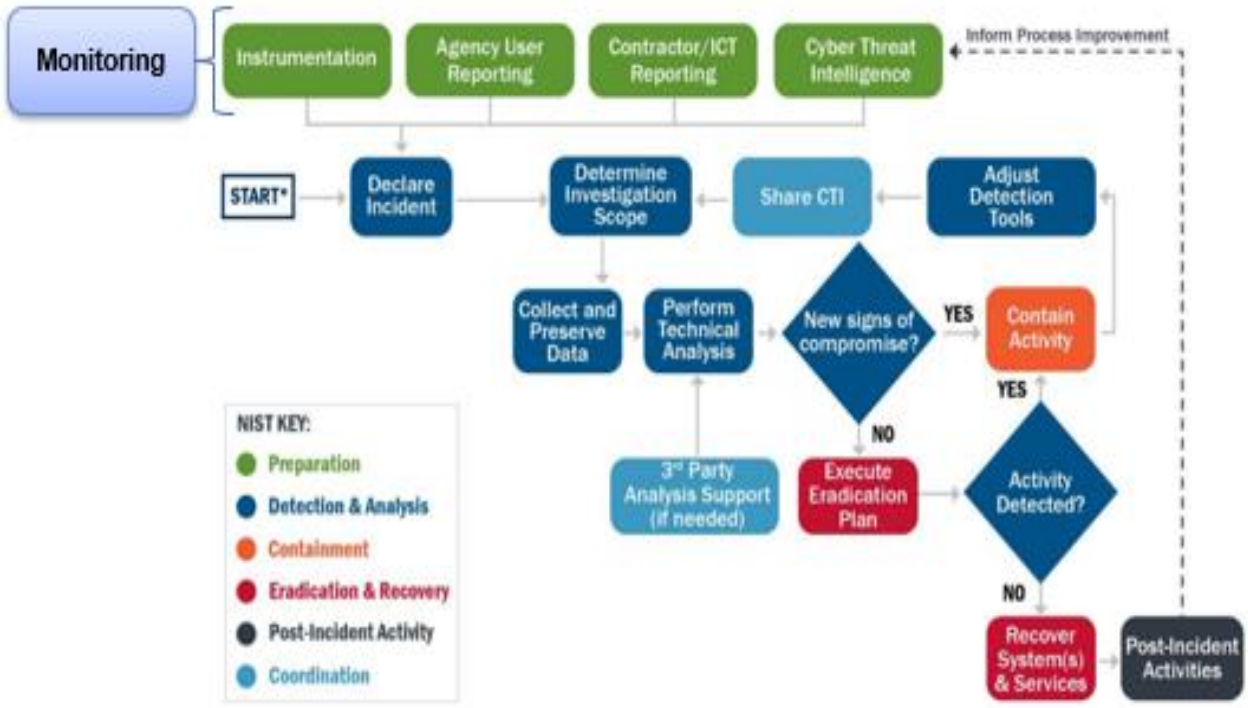
Effective cyber threat detection is critical to prevent and detect cyber incidents before they can cause significant damage (Murphy et al., 2015). However, even the most sophisticated detection technologies cannot guarantee 100% protection against cyber-attacks (Murphy et al., 2015). Hence, to reduce damage and recovery time in the case of a cyber catastrophe, an efficient cyber incident response strategy is crucial (Murphy et al., 2015).

When a threat is detected, the incident response process is initiated to mitigate the impact of the incident (Murphy et al., 2015). It includes a range of activities such as identifying the scope of the incident, containing the incident, restoring systems and data, and conducting post-incident analysis to prevent future incidents (Murphy et al., 2015). An effective incident response plan should include a clear escalation path, defined roles and responsibilities, and communication protocols to ensure that all stakeholders are in the response process (Murphy et al., 2015).

In 2021, CISA released a playbook for responding to cyber incidents to help critical infrastructure sectors like the aviation industry (Hartman, 2021). The playbook has a checklist for responding to an incident and another that can be used to prepare for responding to an incident (Hartman, 2021). Figure 11 shows the cyber incident management activities per the playbook.

Figure 11

Cyberspace Monitoring and Incident Management Activities



Note. The cyberspace monitoring and incident management process. Adapted from *Cybersecurity Incident & Vulnerability Response Playbook*, by CISA, 2021, (https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incide

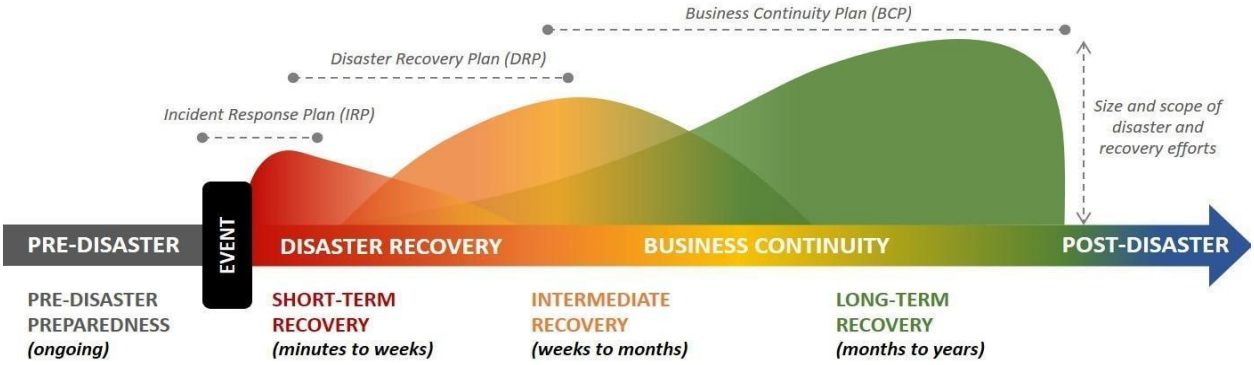
nt_and_Vulnerability_Response_Playbooks_508C.pdf). Copyright 2021 by the Cybersecurity and Infrastructure Security Agency. Adapted with permission.

Similarly, cyber incident management is part of contingency planning, which includes disaster recovery and business continuity planning (Swanson et al., 2010). Disaster recovery planning focuses on restoring critical IT systems and data after a disruptive event, while business continuity planning focuses on maintaining essential business functions in the event of an interruption (Swanson et al., 2010). Integration of these plans is critical to ensuring that organizations can respond to and recover from cyber incidents effectively (Swanson et al., 2010).

For example, a cyber-attack could stop important IT systems from working, which would lead to a disaster recovery scenario (Swanson et al., 2010). In this case, cyber incident management can help identify and contain the incident, while the disaster recovery plan can be used to restore systems and data (Swanson et al., 2010). Business continuity planning can make sure that essential business functions can keep going while the business is getting back on its feet (Swanson et al., 2010). Figure 12 shows how these three plans are integrated and work together.

Figure 12

The Enterprise Continuity Process



Note. The cyber incident response process and enterprise continuity. From *Enterprise Continuity*, 2018, (https://cdn8.bigcommerce.com/s-g93hfm7/product_images/uploaded_images/2018.2-coop-continuity-of-operations-program-phases.jpg). Copyright 2018 by Compliance Forge. Reprinted with permission.

To achieve effective integration, aviation organizations should ensure that their cyber incident management plan is aligned with their disaster recovery and business continuity plans (IBM, 2017). This includes regular testing and simulation exercises to ensure that all plans are coordinated and effective (IBM, 2017). According to IBM (2017), organizations that have a comprehensive cyber incident response plan has an average cost savings of $2.5 million per incident compared to organizations without such plans. By having a comprehensive cyber incident response plan that includes disaster recovery and business continuity planning, aviation organizations can reduce the costs associated with cyber incidents and minimize the damage caused by such incidents (Murphy et al., 2015).

In summary, insider threat monitoring involves the detection and prevention of malicious or unintentional activities by authorized personnel within the aviation organization (Murphy et al., 2015). Malware detection and protection involves the identification and mitigation of malicious software that can disrupt aviation operations (Murphy et al., 2015). Cybersecurity operations involve the implementation and management of security technologies and processes to protect aviation systems and data (Murphy et al., 2015). Cyber incident response involves the response to and recovery from cyber incidents in a timely and effective manner (Murphy et al., 2015).

Together, these four processes form the basis of aviation cyberspace monitoring to protect an organization against cyber threats, minimizing the impact of a security incident and ensuring the continuity of the organization's operations (Murphy et al., 2015). In general, an extensive cybersecurity program must include aircraft cyberspace monitoring (Murphy et al., 2015). By continuously monitoring their systems and networks, aviation organizations can detect and respond to cyber threats in real-time, which is essential to ensuring the safety and security of aviation systems and passengers (Murphy et al., 2015).

Recommendations

Cyber Threat Frameworks

The U.S. aviation industry can improve its cybersecurity practices by using new cyber threat frameworks like MITRE ATT&CK. This framework provides a comprehensive and standardized approach to identifying and categorizing cyber threats, making it easier for organizations to monitor their IT and OT systems for suspicious activity and identify potential threats as they emerge (Goldstein, 2023). Aviation organizations can use the framework, in addition to the Decider tool, to create a baseline understanding of the types of threats they are likely to face based on their specific industry and system architecture (Toulas, 2023).

Using MITRE ATT&CK can also help aviation organizations develop effective defense strategies by mapping known TTPs to specific defensive measures (Goldstein, 2023). This guarantees that they are appropriately protected against the types of cyber threats they are most likely to experience (Goldstein, 2023). The framework can also be used to improve intelligence

sharing and cooperation between aviation organizations when sharing threat intelligence (Toulas, 2023). Aviation organizations can enhance their capacity to recognize and respond to new threats by utilizing a standard vocabulary to define risks and communicate information about TTPs, thereby strengthening their entire cybersecurity posture (Toulas, 2023).

Cyber Threat Detection Technology

In addition to frameworks, the U.S. aviation industry can improve its cybersecurity practices by adopting new cyber threat detection technology. This technology uses AI and ML methods to look for patterns in streaming data that could indicate a cybersecurity event (Stan et al., 2020). Research studies, such as those focused on avionics IDS's that use the ARINC 429 and MIL-STD-1553 communications buses, have shown promising results in detecting possible avionics cyber threats. However, these research projects were limited to a sub-set of avionics systems, small-scale test environments, and without the integration of cyber threat frameworks and SOC functions (Ryon et al., 2020). Due to these restraints, the U.S. aviation industry needs to keep researching new cyber threat detection technology, especially given how quickly IT and OT systems are integrating within the aircraft cyber environment.

Cybersecurity Training for Pilots

And finally, the U.S. aviation industry can improve its cybersecurity practices by improving cybersecurity training and education for pilots and aircrew (Air Line Pilots Association, 2017). Research has been conducted on integrating pilots and in-flight cyber-attacks to develop systems and procedures to help pilots detect, respond to, and recover from cyber incidents while in flight (Gontar et al., 2018). This research has focused on developing human-machine interfaces that provide pilots with real-time information about the aircraft's cyber status

and developing procedures and protocols for pilots to follow in the event of a cyber incident (Gontar et al., 2018). Overall, this research aims to develop systems and procedures that can help pilots detect, respond to, and recover from cyber incidents while in flight, and provide them with the necessary information to make informed decisions about how to respond to these incidents.

Following a similar mandate for railroad owners last year, these new technologies are in line with the Transportation Security Administration's (TSA) new cybersecurity regulations for the aviation industry (Gluley, 2023). Network segmentation, the development of access control measures, the deployment of continuous monitoring and detection, and the reduction of the risk of exploiting unpatched systems are the four steps that TSA-regulated aviation organizations are required to take to minimize cybersecurity threats (Morlando, 2023). Due to the crucial nature of its operations and the potential for severe financial and reputational harm, the aviation industry continues to be a top target for cyber-attacks (Gluley, 2023). Aviation organizations can increase security and better manage their cyber risk by deploying stronger cyberspace monitoring and threat detection.

Conclusion

In the end, this research project shows how important it is for the U.S. aviation industry to have strong cyberspace monitoring and response capabilities to address emerging threats. As technology improves and systems become more connected, cyber-attacks are more likely to happen. The paper emphasizes the need for a multi-layered approach as a means of detecting and responding to cyber threats. Furthermore, the project shows how important it is integrating this

approach with new cybersecurity frameworks and technologies since the cyberspace domain is constantly evolving.

The research project shows what could happen if a cyber-attack on the aviation industry was successful. Such an attack could stop air travel for a long period of time, put the safety of passengers and planes at risk, and do a lot of damage to the economy. This shows how important it is to have strong cybersecurity program, information sharing partnerships, and invest in new cyberspace monitoring capabilities to make them more effective. With these measures, the U.S. aviation industry can better protect against cyber threats and ensure that the aviation cyberspace environment remains safe and secure for all.

Bibliography

Advancing Cyber Resilience in Aviation: An Industry Analysis. World Economic Forum. (2020, January). Retrieved March 2, 2023, from https://www.weforum.org/whitepapers/advancing-cyber-resilience-in-aviation-an-industry-analysis

Ahmed, D. (2020, June 6). *Top US Aerospace services provider suffers breach, loses 1.5 TB of data*. HackRead. Retrieved February 14, 2023, from https://www.hackread.com/us-aerospace-service-provider-breach-data/

Air Line Pilots Association. (2017, June). *Aircraft cybersecurity: The pilot's perspective*. Retrieved April 4, 2023, from https://www.alpa.org/-/media/ALPA/Files/pdfs/news-events/white-papers/white-paper-cybersecurity.pdf?la=en

Alexandrovich, T. (2019). In *Cyber Israel*. Forum of Incident Response and Security Teams. Retrieved February 1, 2023, from https://www.first.org/resources/papers/telaviv2019/INCD-Tom-Alexandrovich-Civil-aviation-cyber-security-threats.pdf.

Alqushayri , D. (2020). *Cybersecurity Vulnerability Analysis and Countermeasures of Commercial Aircraft Avionic Systems* (thesis). Embry Riddle Aeronautical University, Daytona Beach.

Arampatzis, A. (2020, August 9). *The State of Civil Aviation Cybersecurity*. Tripwire. Retrieved January 27, 2023, from https://www.tripwire.com/state-of-security/civil-aviation-cybersecurity

Arampatzis, A. (2021, July 5). *The aviation industry needs to move towards Cyber Resilience*. Tripwire. Retrieved January 27, 2023, from https://www.tripwire.com/state-of-security/aviation-industry-needs-to-move-towards-cyber-resilience

Aratani, L. (2022, October 12). *Hackers knock some U.S. Airport websites offline*. The Washington Post. Retrieved February 12, 2023, from https://www.washingtonpost.com/transportation/2022/10/10/hackers-cyber-attack-airport-websites/

Barrett, M. (2020, January 27). *Framework for improving critical infrastructure cybersecurity version 1.1*. NIST. Retrieved February 16, 2023, from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

Barrett, R. (2022, September 7). *How america's airports defend against cyberthreats*. How America’s Airports Defend Against Cyberthreats. Retrieved February 13, 2023, from https://statetechmagazine.com/article/2022/09/how-americas-airports-defend-against-cyberthreats-perfcon

Barthold, K. (2021, March 4). *Empower your employees to be the first and last line of defense against cyber threats*. Forbes. Retrieved February 12, 2023, from https://www.forbes.com/sites/forbesbusinesscouncil/2021/03/05/empower-your-employees-to-be-the-first-line-of-defense-against-cyber-threats/?sh=ffb803a6f5ae

Be cyber smart: A guide to help you do your part. National Cybersecurity Alliance. (2022, June 14). Retrieved February 4, 2023, from https://staysafeonline.org/online-safety-privacy-basics/be-cyber-smart-a-guide-to-help-you-do-your-part/

Behler, R. (2015). *Cyber-Vulnerabilities in Aviation Today*. Retrieved February 3, 2023, from https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=447923.

Bellamy, W. (2019, July 11). *New computer monitors aircraft network traffic for Cyber Threats*. Avionics International. Retrieved February 19, 2023, from https://www.aviationtoday.com/2019/07/11/new-appliance-monitors-aircraft-network-traffic-cyber-threats/

Berger, D. (2022, July 10). *Defending aircraft networks against cybersecurity breaches*. Tripwire. Retrieved January 27, 2023, from https://www.tripwire.com/state-of-security/defending-aircraft-networks-against-cybersecurity-breaches

Bocetta, S. (2022, November 21). *Aviation starting to get hit with rise of cyberattacks post-pandemic*. Security Boulevard. Retrieved January 31, 2023, from https://securityboulevard.com/2022/11/aviation-starting-to-get-hit-with-rise-of-cyberattacks-post-pandemic/#:~:text=The%20map%20reports%20that%2052,three%2Dquarters%20of%20the%20time.

Brannon, I. (2020, September 22). *Time is running out for lawmakers to save airline industry and jobs*. Forbes. Retrieved February 14, 2023, from https://www.forbes.com/sites/ikebrannon/2020/09/22/time-is-running-out-for-lawmakers-to-save-airline-industry-and-jobs/?sh=55e2c8d85f97

Biesecker, C. (2018, December 13). *AIA issues Baseline Cybersecurity Standards for aerospace and Defense Industry*. Defense Daily. Retrieved February 16, 2023, from https://www.defensedaily.com/aia-issues-baseline-cyber-security-standards-aerospace-defense-industry/cyber/

Bocetta, S. (2022, November 21). *Aviation starting to get hit with rise of cyberattacks post-pandemic*. Security Boulevard. Retrieved February 1, 2023, from https://securityboulevard.com/2022/11/aviation-starting-to-get-hit-with-rise-of-cyberattacks-post-pandemic/#:~:text=The%20map%20reports%20that%2052,three%2Dquarters%20of%20the%20time.

Castagna, R. (2023, January 20). *What is the 3-2-1 backup strategy?* Data Backup. Retrieved February 17, 2023, from https://www.techtarget.com/searchdatabackup/definition/3-2-1-Backup-Strategy

Chaplain, C. (2018, October). *Weapon systems cybersecurity: DoD just beginning to grapple with scale of vulnerabilities*. Weapon Systems Cybersecurity: DoD Just Beginning to Grapple with Scale of Vulnerabilities | U.S. GAO. Retrieved February 6, 2023, from https://www.gao.gov/products/gao-19-128

Cogburn, T. (2022, February). *What is Security Operations (SecOps)? defined, explained, and Trends*. Vation Ventures Research. Retrieved February 17, 2023, from https://www.vationventures.com/research-article/what-is-security-operations

Compliance Forge. (2018). *Enterprise Continuity Process*. Enterprise Continuity. Retrieved March 2, 2023, from https://cdn8.bigcommerce.com/s-g93hfm7/product_images/uploaded_images/2018.2-coop-continuity-of-operations-program-phases.jpg.

Corretjer, P. J. (2018, January 1). *A cybersecurity analysis of today's commercial aircrafts and aviation industry systems*. NASA/ADS. Retrieved January 27, 2023, from https://ui.adsabs.harvard.edu/abs/2018MsT.....22C/abstract

Costa, D. (2017, March 7). CERT Definition of 'Insider Threat' - Updated. Retrieved March 1, 2023, from http://insights.sei.cmu.edu/blog/cert-definition-of-insider-threat-updated/.

Cybersecurity and Infrastructure Security Agency, & Hartman, M., Cybersecurity Incident & Vulnerability Response Playbooks 1–43 (2021). Washington , DC; Cybersecurity and Infrastructure Security Agency.

Daivanayagam, S. (2021, May 24). *Airports to be fastest-growing critical infrastructure sector to invest in cybersecurity by 2030*. Frost & Sullivan. Retrieved February 13, 2023, from https://www.frost.com/news/press-releases/airports-to-be-fastest-growing-critical-infrastructure-sector-to-invest-in-cybersecurity-by-2030/#:~:text=%E2%80%9CWhile%20oil%20and%20gas%20facilities,for%20Security%20at%20Frost%20%26%20Sullivan.

Dave, G., Choudhary, G., Sihag, V., You, I., & Choo, K.-K. R. (2022). Cybersecurity challenges in aviation communication, navigation, and surveillance. *Computers & Security*, *112*, 102516. https://doi.org/10.1016/j.cose.2021.102516

David , A. (2021, June 9). Aviation Cyber-Security Regulation: Introduction to the DO-326/ED-202-set. Retrieved February 16, 2023, from https://afuzion.com/do-326a-ed-202a-aviation-cyber-security/

David, A. (2021). Unsettled topics concerning airport cybersecurity standards and regulation. https://doi.org/10.4271/epr2021020

De Moura, G., Merritt, J., Uppink, L., Wylde, G., Coman, L., De Landtsheer, C., Fichtinger, I., & Verdonck, C. (2021, April). *Pathways towards a cyber resilient aviation industry*. World Economic Forum. Retrieved February 3, 2023, from https://www.weforum.org/reports/pathways-towards-a-cyber-resilient-aviation-industry

Dickson, S. (2020, October). *A Report on the History, Current Status, and Future of National Airspace System Modernization* . NextGen Annual Report Fiscal Year 2020. Retrieved February 14, 2023, from https://www.faa.gov/sites/faa.gov/files/2022-06/NextGenAnnualReport-FiscalYear2020.pdf

Dorais-Joncas, A., & Muñoz, F. (2022, January 11). *Jumping the air gap: 15 years of Nation-state effort*. WeLiveSecurity. Retrieved February 19, 2023, from https://www.welivesecurity.com/2021/12/01/jumping-air-gap-15-years-nation-state-effort/

Dulavitz, M. (2019, March 28). *Strengthen security of your data center with the NIST Cybersecurity Framework*. Dell. Retrieved February 19, 2023, from https://www.dell.com/en-us/blog/strengthen-security-of-your-data-center-with-the-nist-cybersecurity-framework/

Edwards, J. (2021, June 21). *7 ways technical debt increases security risk.* CSO Online. Retrieved February 14, 2023, from https://www.csoonline.com/article/3621754/7-ways-technical-debt-increases-security-risk.html

European Organization for the Safety of Air Navigation. (2021, July). *Eurocontrol Think Paper #12 - aviation under attack from a wave of cybercrime*. EUROCONTROL. Retrieved January 31, 2023, from https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime

Flessas, C. (2022, August 3). *Aviation safety and cybersecurity: Learning from incidents*. Tripwire. Retrieved January 27, 2023, from https://www.tripwire.com/state-of-security/aviation-safety-cybersecurity-learning-from-incidents

Fox, S. J. (2016). Flying challenges for the future: Aviation preparedness – in the face of cyber-terrorism. *Journal of Transportation Security*, *9*(3-4), 191–218. https://doi.org/10.1007/s12198-016-0174-1

Federal Aviation Administration. (2021, January). *Aerospace forecast fiscal years 2021-2041*. Newsroom . Retrieved February 14, 2023, from https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=26935

Federal Communications Commission. (2020). *Cybersecurity Tips for International Travelers*. Washington , DC; Consumer and Governmental Affairs Bureau ·.

Francy, F. (2015). The aviation information sharing and analysis center (A-ISAC). *2015 Integrated Communication, Navigation and Surveillance Conference (ICNS)*. https://doi.org/10.1109/icnsurv.2015.7121274

Gates, M. (2020, March 1). *Enhancing in-flight cybersecurity*. ASIS Homepage. Retrieved February 13, 2023, from https://www.asisonline.org/security-management-magazine/articles/2020/03/enhancing-in-flight-cybersecurity/

Georgios, L. (2022, March). *Cybersecurity considerations for Aerial Networks*. International Hellic University. Retrieved January 27, 2023, from https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/29950/IHU_SciTech_Thesis_CyberSecurity%20Considerations%20for%20Aerial%20Networks_Limnaios_George.pdf?sequence=1

Gillum, J., & Woodhouse, S. (2022, October 10). *Pro-Russian hacktivists claim credit for attacks on airport websites*. Bloomberg. Retrieved February 12, 2023, from https://www.bloomberg.com/news/articles/2022-10-10/pro-russian-hacktivists-claim-credit-for-attacks-on-airport-websites

Global Industry Analysts. (2022, March 23). *Valued to be $5.9 billion by 2026, in-flight wi-fi slated for robust growth worldwide*. Valued to be $5.9 Billion by 2026, In-Flight Wi-Fi Slated for Robust Growth Worldwide. Retrieved February 14, 2023, from https://www.prnewswire.com/news-releases/valued-to-be-5-9-billion-by-2026--in-flight-wi-fi-slated-for-robust-growth-worldwide-301506339.html

Gluley, G. (2023, March 9). *TSA tells us aviation industry to boost its cybersecurity*. Tripwire. Retrieved April 4, 2023, from https://www.tripwire.com/state-of-security/tsa-tells-us-aviation-industry-boost-its-cybersecurity

Godlewski, M. (2022, November 11). *Cyber Incident Affects Electronic Flight Bag Users*. Flying Magazine. Retrieved February 12, 2023, from https://www.flyingmag.com/cyber-incident-affects-electronic-flight-bag-users/

Goldstein, E. (2023, March 31). *CISA releases best practice guidance to help organizations map adversary behavior to MITRE ATT&CK Framework*. Cybersecurity and Infrastructure Security Agency CISA. Retrieved April 2, 2023, from https://www.cisa.gov/news-events/news/cisa-releases-best-practice-guidance-help-organizations-map-adversary-behavior

Gontar, P., Homans, H., Rostalski, M., Behrend, J., Dehais, F., & Bengler, K. (2018, May 31). *Are pilots prepared for a cyber-attack? A human factors approach to the experimental*

evaluation of pilots' behavior. Journal of Air Transport Management. Retrieved February 19, 2023, from https://trid.trb.org/view/1510991

Goodwyn, W. (2012, October 29). *Sandy shuts down nine airports along East Coast*. National Public Radio. Retrieved February 12, 2023, from https://www.npr.org/2012/10/29/163896131/sandy-shuts-down-nine-airports-along-east-coast

Greenberg, A. (2018, August 22). *The untold story of notpetya, the most devastating cyberattack in history*. Wired. Retrieved February 24, 2023, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greig, J. (2023, January 17). *Congressman calls on CISA to investigate air travel vulnerabilities after outage*. The Record from Recorded Future News. Retrieved February 7, 2023, from https://therecord.media/congressman-calls-on-cisa-to-investigate-air-travel-vulnerabilities-after-outage/#:~:text=Malware-,Congressman%20calls%20on%20CISA%20to%20investigate%20air%20travel%20vulnerabilities%20after,crippled%20flights%20across%20the%20country.

Grossman, L. (2021, December 2). *Before the United States House of Representatives Committee on Transportation and Infrastructure: The Evolving Cybersecurity Landscape: Federal Perspectives on securing the nation's infrastructure*. Before The United States House Of Representatives Committee On Transportation And Infrastructure: The Evolving Cybersecurity Landscape: Federal Perspectives On Securing The Nation's Infrastructure | Federal Aviation Administration. Retrieved February 14, 2023, from

https://www.faa.gov/testimony/united-states-house-representatives-committee-transportation-and-infrastructure-evolving

Harris, M. (2022, November 22). *FAA fumbled its response to a surge in GPS jamming*. IEEE Spectrum. Retrieved February 19, 2023, from https://spectrum.ieee.org/gps-jamming

Hampton , M. (2020, September 2). *FAA and its partner agencies have begun work on the Aviation Cyber Initiative and are implementing priorities*. The U.S. Department of Transportation. Retrieved February 14, 2023, from https://trid.trb.org/view/1740413

Hartmann, M. (2023). (rep.). *Best Practices for MITRE ATT&CK Mapping*. Cybersecurity and Infrastructure Security Agency. Retrieved February 1, 2023, from https://www.cisa.gov/uscert/sites/default/files/publications/Best%20Practices%20for%20MITRE%20ATTCK%20Mapping.pdf.

Holden, R., Lee, X., Longoria, P., Prediger, S., Tonti, S., de Rodriguez, L., & Woolson, M. (2018, January). Quick Guide for Airport Cybersecurity. Retrieved February 17, 2023, from https://www.sskies.org/images/uploads/subpage/PARAS_0007.CybersecurityQuickGuide.FinalReport.pdf

Holemans, L. (2022). *Federal Aviation Administration ATO Cybersecurity Working Group*. Cybersecurity Awareness Symposium . Retrieved February 2023, from https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cas/acg/acg1.pdf

Holemans, L. (2022, June 9). *The FAA moves to Zero Trust Strategy for Preventing Cyber Attacks*. Connected Aviation Intelligence. Retrieved February 3, 2023, from https://www.gcasummit.com/the-faa-moves-to-zero-trust-strategy-for-preventing-cyber-attacks/

IBM. (2017, July 8). *IBM, Ponemon: Business Continuity Management helps save time and cost*. Dark Reading. Retrieved February 20, 2023, from https://www.darkreading.com/cloud/ibm-ponemon-business-continuity-management-helps-save-time-and-cost-post-breach

Inmarsat Aviation. (2017). *Air Travelers See Inflight Broadband as an essential freedom*. Inmarsat Aviation. Retrieved February 19, 2023, from https://www.inmarsat.com/en/insights/aviation/2017/air-travellers-see-inflight-broadband-as-an-essential-freedom.html

International Air Transport Association . (2021, December). *Compilation of cybersecurity regulations, standards, and guidance*. Compilation of Cybersecurity Regulations, Standards, and Guidance Applicable to Civil Aviation version 3.0. Retrieved February 16, 2023, from https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilation-of-cyber-regulations-standards-and-guidance_3.0.pdf

Iyengar, R. (2022, September 3). *How airlines give you internet access at 35,000 feet - and why it still needs a lot of work | CNN business*. CNN. Retrieved February 14, 2023, from https://www.cnn.com/2022/09/03/tech/inflight-wifi-technology/index.html

Janofsky, A. (2022, November 3). *Cyber incident at Boeing subsidiary causes flight planning disruptions*. The Record from Recorded Future News. Retrieved February 7, 2023, from https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions/

J. Cano M.,, J. (2019, October). *The human factor in information security*. ISACA. Retrieved February 4, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2019/volume-5/the-human-factor-in-information-security

Janofsky, A. (2022, November 3). *Cyber incident at Boeing subsidiary causes flight planning disruptions*. The Record from Recorded Future News. Retrieved February 12, 2023, from https://therecord.media/cyber-incident-at-boeing-subsidiary-causes-flight-planning-disruptions/

Kaliyaperumal, L. N. (2021, October). *The evolution of security operations and strategies for building an effective SOC*. ISACA. Retrieved February 17, 2023, from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-5/the-evolution-of-security-operations-and-strategies-for-building-an-effective-soc

Kessler, G. C., & Craiger, J. P. (n.d.). *Aviation cybersecurity: An overview*. Scholarly Commons. Retrieved January 27, 2023, from https://commons.erau.edu/ntas/2018/presentations/37

Kölle, R., Markarian, G., & Tarter, A. (2011). *Aviation security engineering a holistic approach*. Artech House.

Klim, Z., & Skorek, A. (2019). Hawaii University International Conferences. In *Cybersecurity Risk Assessment for the Continuing Airworthiness* (pp. 1–14). Honolulu, HI; Hawaii University International Conferences.

Knerler, K., Knerler, K., Parker, I., & Zimmerman, C. (2022, March 31). *11 strategies of a world-class cybersecurity operations center*. MITRE. Retrieved February 17, 2023, from https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center

Koroniotis, N., Moustafa, N., Schiliro, F., Gauravaram, P., & Janicke, H. (2020). A holistic review of cybersecurity and Reliability Perspectives in smart airports. *IEEE Access, 8,* 209802–209834. https://doi.org/10.1109/access.2020.3036728

Kostka, C. (2022, August 16). *Aviation industry at risk from Ransomware*. Ransomware.org. Retrieved February 14, 2023, from https://ransomware.org/blog/aviation-industry-at-risk-from-ransomware/

Kotler, I. (2022, February 28). *Making the world a safer place through (cyber) hygiene*. Forbes. Retrieved February 12, 2023, from https://www.forbes.com/sites/forbestechcouncil/2022/02/25/making-the-world-a-safer-place-through-cyber-hygiene/?sh=5ddb45851d7f

Koziol, J., & Bottorff, C. (2022, June 13). *Cybersecurity awareness: What it is and how to start*. Forbes. Retrieved February 12, 2023, from https://www.forbes.com/advisor/business/what-is-cybersecurity-awareness/

Krause, H., & Marinos, N. (2020). (rep.). *Aviation Cybersecurity: FAA Should Fully Implement Key Practices to Strengthen Its Oversight of Avionics Risks*. The United States Government Accountability Office. Retrieved February 1, 2023, from https://www.gao.gov/assets/gao-21-86.pdf.

Kumpf, K. (2023, January 17). *What the FAA outage reveals about the state of critical infrastructure*. Security Boulevard. Retrieved February 14, 2023, from https://securityboulevard.com/2023/01/what-the-faa-outage-reveals-about-the-state-of-critical-infrastructure/

Kuzio de Naray, R., Haugh, B., & Wartik, S. (2022). (rep.). *An Ontology for the Embedded System Threat Matrix* (pp. 1–37). Alexandria, VA: Institute for Defense Analysis.

Kölle, R., Markarian, G., & Tarter, A. (2011). *Aviation security engineering a holistic approach*. Artech House.

Lopamudra, M. (2017, April 4). *Airbus and Sita Launch Security Operations Center services for Air Transport Industry*. Airport Technology. Retrieved February 17, 2023, from https://www.airport-technology.com/news/newsairbus-launches-sitas-latest-cybersecurity-services-for-air-transport-industry-5778179/

Luci, H. (2020). *Cybersecurity Roles & Responsibilities*. 2020 FAA Cybersecurity Awareness Symposium. Federal Aviation Administration. Retrieved February 3, 2023, from https://www.faa.gov/sites/faa.gov/files/air_traffic/technology/cas/acg/acg1.pdf.

Lykou, G., Anagnostopoulou, A., & Gritzalis, D. (2018). Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors*, *19*(1), 19. https://doi.org/10.3390/s19010019

Mahn, A., Topper, D., Quinn, S., & Marron, J. (2022, November 29). *Getting started with the NIST Cybersecurity Framework: A quick start guide*. NIST. Retrieved February 3, 2023, from https://www.nist.gov/publications/getting-started-nist-cybersecurity-framework-quick-start-guide

Mariani, J., Zmud, J., & Krimmel, E. (2019, July). *Flying smarter - The smart airport and the Internet of Things*. Deloitte Insights. Retrieved February 13, 2023, from https://www2.deloitte.com/us/en/insights/industry/public-sector/iot-in-smart-airports.html

Mayorkas, A. (2022, October). *DHS announces New Cybersecurity performance goals for Critical Infrastructure* . DHS Announces New Cybersecurity Performance Goals for Critical Infrastructure . Retrieved February 6, 2023, from

https://www.dhs.gov/news/2022/10/27/dhs-announces-new-cybersecurity-performance-goals-critical-infrastructure

McCollum, M. (2020, August 11). *"Zero Trust" Strengthens Aviation Cybersecurity*. MITRE. Retrieved February 3, 2023, from https://www.mitre.org/news-insights/impact-story/zero-trust-strengthens-aviation-cybersecurity

Miller, J., Jimroglou, N., Farol, R., & Hancock, D. (2021, June). Cybersecurity Operations Report - Denver International Airport. Retrieved February 17, 2023, from https://denvergov.org/files/assets/public/auditor/documents/audit-services/audit-reports/2021/den-soc-public-follow-up-report.pdf

Mitchell, R., & Chen, I.-R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys*, *46*(4), 1–29. https://doi.org/10.1145/2542049

Monteagudo, J. (2022, September 19). *Aviation cybersecurity - understanding the airport ecosystem*. The Cyber Startup Observatory. Retrieved February 13, 2023, from https://cyberstartupobservatory.com/aviation-cyber-security-understanding-the-airport-ecosystem/

Montgomery, M., & Ma, J. (2022, November 22). No room for half-measures in aviation cybersecurity. Retrieved February 6, 2023, from https://www.fdd.org/analysis/2022/11/22/no-half-measures-aviation-cybersecurity/#:~:text=TSA%20faced%20industry%20pushback%20when,to%20CISA%20within%2024%20hours.

Moon, M. (2023, January 14). *FAA's NOTAM computer outage affected military flights*. Engadget. Retrieved February 11, 2023, from https://www.engadget.com/faa-notam-computer-outage-affected-even-military-flights-155514704.html

Moore, J. (2012, October 31). *Superstorm Sandy Floods East Coast Airports*. Aircraft Owners and Pilots Association. Retrieved February 12, 2023, from https://www.aopa.org/news-and-media/all-news/2012/october/31/superstorm-sandy-floods-east-coast-airports

Morlando, S. (2023, March 22). *A closer look at TSA's new cybersecurity requirements for Aviation*. Help Net Security. Retrieved April 4, 2023, from https://www.helpnetsecurity.com/2023/03/23/aviation-industry-cybersecurity-requirements/

Muntean, P., & Wallace, G. (2023, January 12). *FAA system outage causes thousands of flight delays and cancellations across the US*. CNN. Retrieved February 11, 2023, from https://www.cnn.com/travel/article/faa-computer-outage-flights-grounded/index.html

Murphy, R. J., Sukkarieh, M., Haass, J., & Hriljac, P. M. (2015). *Guidebook on best practices for airport cybersecurity*. Transportation Research Board.

Myers, A. (2022, November 17). *Cyber incident impacts Boeing subsidiary Jeppesen's flight planning tools*. Avionics International. Retrieved February 12, 2023, from https://www.aviationtoday.com/2022/11/16/cyber-incident-impacts-boeing-subsidiary-jeppesens-flight-planning-tools/

Naumann, D. (2021). *Five ways 5G will change the air travel experience*. Verizon Enterprise. Retrieved February 19, 2023, from https://www.verizon.com/business/resources/articles/five-ways-5g-will-transform-the-air-travel-experience/

Nobles, C. (2018). Cyber threats in civil aviation. *Cybersecurity and Threats*, 1185–1207. https://doi.org/10.4018/978-1-5225-5634-3.ch058

Nweke, L. O. (2021). A survey of specification-based intrusion detection techniques for cyber-physical systems. *International Journal of Advanced Computer Science and Applications, 12*(5). https://doi.org/10.14569/ijacsa.2021.0120506

Pathan, A.-S. K. (2020). *Securing Cyber-Physical Systems*. CRC PRESS.

Pecharromán, J. M. P. (2021, October). ICAO Aviation Cybersecurity Strategy. Retrieved February 16, 2023, from https://www.icao.int/NACC/Documents/Meetings/2021/CSWATM/P01-CYBERWEBINAR-ICAOnacc.pdf

Phillips, P. (2022, August 8). Aviation is facing a rising wave of cyber-attacks in the wake of COVID. Retrieved February 6, 2023, from https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid

Phillips, P., Champion, J., & Bettle, P. (2022, August 8). Aviation is facing a rising wave of cyber-attacks in the wake of COVID. Retrieved February 12, 2023, from https://www.shlegal.com/insights/aviation-is-facing-a-rising-wave-of-cyber-attacks-in-the-wake-of-covid

Rayome, A. D. N., Abdullahi, A., Shacklett, M., Greenberg, K., & Stone, B. (2018, July 18). *The 10 airports where your phone is most likely to get hacked*. TechRepublic. Retrieved February 13, 2023, from https://www.techrepublic.com/article/the-10-airports-where-your-phone-is-most-likely-to-get-hacked/

Reed, J. (2022, June 17). *The FAA moves to Zero trust strategy for preventing cyber attacks*. Via Satellite. Retrieved February 3, 2023, from https://www.satellitetoday.com/cybersecurity/2022/06/17/the-faa-moves-to-zero-trust-strategy-for-preventing-cyber-attacks/

Rexroth, A. (2018, July 2). *RTCA examines GPS interference training impacts*. Aviation International News. Retrieved February 19, 2023, from https://www.ainonline.com/aviation-news/general-aviation/2018-07-02/rtca-examines-gps-interference-training-impacts

Ricker, T. (2017). Avionics bus technology: Which bus should I get on? *2017 IEEE/AIAA 36th Digital Avionics Systems Conference (DASC)*. https://doi.org/10.1109/dasc.2017.8102152

Rockwell Collins. (2016, October 13). *Aviation Cybersecurity Research*. Aviation Week Network. Retrieved February 16, 2023, from https://aviationweek.com/knowledge-center/aviation-cybersecurity-research

Rohith, C., & Kaur, G. (2021). A comprehensive study on malware detection and prevention techniques used by anti-virus. *2021 2nd International Conference on Intelligent Engineering and Management (ICIEM)*. https://doi.org/10.1109/iciem51511.2021.9445322

Ryon, L., Rice, G., & Potts, J. (2020). An avionics cyber intrusion detection system. *AIAA Scitech 2020 Forum*. https://doi.org/10.2514/6.2020-0318

Sampigethaya, K. (2019). Aircraft Cybersecurity Risk Assessment: Bringing Air Traffic Control and cyber-physical security to the forefront. *AIAA Scitech 2019 Forum*. https://doi.org/10.2514/6.2019-0061

Schaufele , R. (2020, January). *The Economic Impact of Civil Aviation on the U.S. Economy*. Federal Aviation Administration. Retrieved February 14, 2023, from https://www.faa.gov/about/plans_reports/media/2020_jan_economic_impact_report.pdf

Sezari, B., Moller, D. P., & Deutschmann, A. (2018). Anomaly-based network intrusion detection model using deep learning in airports. *2018 17th IEEE International*

Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE). https://doi.org/10.1109/trustcom/bigdatase.2018.00261

Shahzad Haroon, M., & Mansoor Ali, H. (2022). Adversarial training against adversarial attacks for machine learning-based Intrusion Detection Systems. *Computers, Materials & Continua*, *73*(2), 3513–3527. https://doi.org/10.32604/cmc.2022.029858

Shead, S. (2022, June 27). *Hackers can bring ships and planes to a grinding halt. and it could become much more common*. CNBC. Retrieved February 19, 2023, from https://www.cnbc.com/2022/06/27/hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html

Sheble, M. (2020, October). *How GDPR will affect the aviation industry*. LinkedIn. Retrieved February 16, 2023, from https://www.linkedin.com/pulse/how-gdpr-affect-aviation-industry-matthew-sheble/

Shepardson, D. (2020, April 6). *Alaska air carrier RavnAir files for bankruptcy as U.S. Treasury mulls grants*. Reuters. Retrieved February 14, 2023, from https://www.reuters.com/article/health-coronavirus-usa-airlines-idUSL1N2BU102

Shepardson, D. (2022, October 12). *U.S. to issue new cybersecurity requirements for Critical Aviation Systems*. Reuters. Retrieved February 4, 2023, from https://www.reuters.com/world/us/us-issue-new-cybersecurity-requirements-critical-aviation-systems-2022-10-12/

Shepardson, D. (2022, October 25). *Exclusive: FAA warns of Aviation Safety Risks without U.S. mandate on 5G limits*. Reuters. Retrieved February 14, 2023, from

https://www.reuters.com/business/aerospace-defense/exclusive-faa-sees-aviation-safety-risks-without-us-telecom-agency-mandate-2022-10-25/

Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T. J., & Flynn, L. (2018). Common Sense Guide to Mitigating Insider Threats, Sixth Edition. *CERT National Insider Threat Center*. https://doi.org/10.21236/ada585500

Sinnatt, J., & Haq, R. (2017, July 31). *Inmarsat survey shows 60% believe in-flight wi-fi is a necessity*. Avionics International. Retrieved February 14, 2023, from https://www.aviationtoday.com/2017/07/31/inmarsat-survey-shows-60-believe-inflight-wi-fi-necessity/

Smith, M., Strohmeier, M., Harman, J., Lenders, V., & Martinovic, I. (2019, May 20). *Safety vs. security: Attacking avionic systems with humans in the loop*. arXiv.org. Retrieved February 7, 2023, from https://arxiv.org/abs/1905.08039

Strom, B., Strom, B., Applebaum, A., Miller, D., Nickels, K., Pennington, A., & Thomas, C. (2020, March 31). *Mitre ATT&CK: Design and philosophy*. MITRE. Retrieved February 19, 2023, from https://www.mitre.org/news-insights/publication/mitre-attck-design-and-philosophy

Swanson, M., Bowen , P., Phillips , A., Gallup , D., & Lynes , D. (2010, May). *Contingency planning guide for federal information systems* . Contingency Planning Guide for Federal Information Systems . Retrieved February 20, 2023, from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

Thames, L. (2015, June 23). *Did the Aviation Industry Fail Cybersecurity 101?* Tripwire. Retrieved January 27, 2023, from https://www.tripwire.com/state-of-security/the-aviation-industry-did-they-fail-cybersecurity-101

Thomson, I. (2013, August 12). *Feds arrest rogue trucker after GPS jamming borks New Jersey Airport Test*. Feds arrest rogue trucker after GPS jamming borks New Jersey airport test. Retrieved February 19, 2023, from https://www.theregister.com/2013/08/12/feds_arrest_rogue_trucker_after_gps_jamming_disrupts_newark_airport/

Toulas, B. (2023, March 2). *CISA releases free 'decider' tool to help with MITRE ATT&CK mapping*. Bleeping Computer. Retrieved April 2, 2023, from https://www.bleepingcomputer.com/news/security/cisa-releases-free-decider-tool-to-help-with-mitre-attandck-mapping/

Tiwari, S. (2022, June). *Travel-related cybercrime takes off as industry rebounds*. Travel-related Cybercrime Takes Off as Industry Rebounds. Retrieved February 4, 2023, from https://threatpost.com/travel-related-cybercrime-takes-off/179962/

Tunčikienė, Ž., & Katinas, R. (2020). Solutions for improving the partnership between Airport and airline companies. *Business, Management and Education*, *18*(2), 247–264. https://doi.org/10.3846/bme.2020.12712

Ukwandu, E., Ben-Farah, M. A., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security challenges in aviation industry: A review of current and future trends. *Information*, *13*(3), 146. https://doi.org/10.3390/info13030146

U.S. Department of Homeland Security. (2021). *If You See Something, Say Something*. Washington, DC; Department of Homeland Security. Retrieved February 4, 2023, from https://www.dhs.gov/sites/default/files/publications/SeeSay-Overview508_1.pdf.

U.S. Department of Homeland Security. (2018, December). *National Strategy for Aviation Security*. The Homeland Security Digital Library. Retrieved February 14, 2023, from https://www.hsdl.org/c/view?docid=821736

Vaughan, M. (2020, January). *Cyber resilience in the aviation industry*. Advancing Cyber Resilience in Aviation: An Industry Analysis. Retrieved February 14, 2023, from https://www3.weforum.org/docs/WEF_Cyber_Resilience_in_the_Aviation_Industry.pdf

Wallace, G., Lyngaas, S., Muntean, P., & Watson, M. (2022, October 10). *Russian-speaking hackers knock multiple US airport websites offline. no impact on operations reported*. CNN. Retrieved February 12, 2023, from https://www.cnn.com/2022/10/10/us/airport-websites-russia-hackers/index.html

Watson, W. T. (2020, January). *Advancing Cyber Resilience in Aviation: An Industry Analysis*. World Economic Forum. Retrieved February 1, 2023, from https://www.weforum.org/whitepapers/advancing-cyber-resilience-in-aviation-an-industry-analysis/

Weinelt, B., & Moavenzadeh, J. (2017, January). Digital Transformation Initiative Aviation, Travel and Tourism Industry. Retrieved February 3, 2023, from https://www3.weforum.org/docs/IP/2017/MO/WEF_ATT_DigitalBorders_WhitePaper.pdf

Welch, P. (2017, January). *AF looks to ensure cyber resiliency in weapons systems through New Office*. AF looks to ensure cyber resiliency in weapons systems through new office. Retrieved February 6, 2023, from https://www.af.mil/News/Article-Display/Article/1041426/af-looks-to-ensure-cyber-resiliency-in-weapons-systems-through-new-office/

Wolfe, F. (2020, April 29). *FAA, EASA Clarify Avionics Mandates to meet Cybersecurity Challenge*. Aviation Today. Retrieved February 1, 2023, from https://interactive.aviationtoday.com/faa-easa-clarify-avionics-mandates-to-meet-cybersecurity-challenge/

Zetter, K. (2015, May 16). *Feds say that banned researcher commandeered a plane*. Wired. Retrieved February 2, 2023, from https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/

Zmud, J., Miller, M., Moran, M., Tooley, M., Borowiec, J., Brydia, B., Sen, R., Mariani, J., Krimmel, E., & Gunnels, A. (2018). A primer to prepare for the Connected Airport and the internet of things. https://doi.org/10.17226/25299

Zuniga, M., & Janson, M. (2022). (tech.). *Platform Independent Vectors of Techniques (PIVOT) - An Approach for System-of-System Attack Path Analysis* (pp. 1–6). Dayton, OH: MITRE.