Journal of Transportation Security (2024) 17:13
https://doi.org/10.1007/s12198-024-00281-9

REVIEW

The types of hackers and cyberattacks in the aviation industry

Lázaro Florido-Benítez[1]

Received: 27 March 2024 / Accepted: 18 July 2024

Abstract

The main goal of this study is to analyse the types of hackers and cyberattacks in the aviation industry, to enhance cybersecurity in the air sector. This manuscript has identified 12 different typologies of hackers in the aviation context. First, those hackers who exercise responsibility in proper, effective, ethical, and good practices to improve the safety of citizens and organizations, such as white unicorns, red, blue, green, and nation sponsored hackers. And second, those hackers that are developing and using cyberattacks with bad practices to provoke serious material damage to public and private organizations, consumers, or even terrorist acts to kill people, including black, nation-state, cyberterrorist, whistle-blower, hacktivist, script kiddie, and gray hackers. Furthermore, findings reveal 54 cyberattacks documented in the period analysed (2000 – January 2024). Of the total cyberattacks in the period analysed, 35 were perpetrated at airports (65%) and 19 by airlines (35%). This study also suggests some lines of action to ensure and guarantee the security of data and private information for business-to-consumer (B2C) and business-to-business (B2B) and their transactions in the aviation industry.

Keywords Cyberattacks · Hackers · Typology · Motivations · Cybersecurity · Airports · Airlines · Aviation industry

Introduction

The aviation industry covers a broad spectrum of stakeholders, including airlines, airports, technology providers, logistics operators, retail companies, tourism companies, and national and regional governments. Indeed, an airport is a critical infrastructure that must protect the safety, social, and economic prosperity of regions and countries (Florido-Benítez 2023a; El-Maissi et al. 2023). Noteworthy, the

✉ Lázaro Florido-Benítez
lfb@uma.es

[1] Department of Economics and Business Administration, University of Málaga, 29016 Málaga, Spain

Published online: 28 August 2024

cornerstone and success of large companies such as Amazon, Zara, JD.com, Alibaba, eBay, or Rakuten lie mainly in creating innovative products and services supported by airports, air cargo, and logistic operators to deliver their orders within three days (Florido-Benítez and Aldeanueva Fernández 2022; Florido-Benítez 2023b). Air cargo operations are observed as an efficient means of transportation for companies and consumers because of their capacity to handle high-value and time-sensitive goods (Adenigbo et al. 2023). Moreover, in both passenger and monetary terms, the European airports lost 1.32 billion passengers and €33.6 billion in passenger revenue because of coronavirus crisis in 2020 (Parliament 2021). Therefore, the aviation industry plays an important role in the movement of tourists to tourist destinations, logistic and e-commerce companies, and consumers.

Safety and cybersecurity are the top priorities in the air transport sector, and the use of disruptive technologies should not compromise operational and commercial activities. Nevertheless, the air transport industry was one of the main targets for hackers in 2022 (KonBriefing. 2022), and 62% of airport authorities reported that their airports were targets of cyberattacks in 2021 (ACI 2021). In 2020, the European Aviation Safety Agency (EASA) estimated a monthly average of 1,000 airport cyberattacks (EASA 2021). 1 hour of operations disruption at a large airport at peak time has an estimated cost of $1million; in fact, the cost of a cyberattack is estimated at around $1million in an airport (Airbus. 2020). A cyberattack is an illegal action that directly affects airports and airlines' operations, their corporate image, reputation, reliability, and passengers' confidence. The global aviation cybersecurity market size reached $4.6 billion in 2023, and it is expected to reach $8 billion by 2032 (IMARC Group 2024).

On January 7, 2023, a cyberattack hit the Beirut-Rafic Hariri airport in Lebanon. On the airport's screens, passengers could read that the arms smuggling would lead to the bombing of the airport and that Hezbollah and Iran are taking the country to war (Paganini 2024). There are not 100 percent safe spaces, the risk of a cyberattack is always latent (Florido-Benítez 2021). According to the International Air Transport Association (IATA) (IATA 2023) reported that cyberattacks are increasing in the aviation industry, and airport and airline operators must comply with aviation cybersecurity regulations across the world.

The economic impact of cybercrime on business is predicted to reach $10.5 trillion by 2025 (Willard 2023). The potential for cyberattacks on the aviation industry is a pressing issue requiring constant attention and proactive measures. Unauthorized access is the most prominent type of cyberattack in the aviation industry to steal intellectual property, intelligence, and private information (Ukwandu et al. 2022). The air transport industry faces increased cyberthreats and cyberattacks due to hyperconnectivity and the lack of standardized frameworks and cybersecurity defences (Nobles 2019).

There are different types of cyberattacks and hackers, so there is a need to be aware of such attacks to protect and analyse the air transport sector from hackers (Biju et al. 2019), and to identify new threats and attacks on different levels of the air transport industry (Sangwan et al. 2023). Ahsan et al. (Ahsan et al. 2022) suggest that historical network data and a machine learning model can prevent cyberattacks and design intelligent security systems against future cyberthreats. There are limited

scientific publications that address the types of hackers and cyberattacks in the aviation industry context (Florido-Benítez 2021; Ukwandu et al. 2022; Kagalwalla and Churi 2019; Suciu et al. 2018; Chng et al. 2022) in order to improve the cybersecurity of airports and airlines' operational and logistic activities. Moving from these considerations and gaps, the main goal of this study is to analyse the types of hackers and cyberattacks in the aviation industry, to enhance cybersecurity in the air sector. Analysing cyberattacks enables researchers and airport and airline operators to identify hackers' motivations, characteristics, and types of cyberattacks in air transport (Lehto 2020). Greater efforts are required in the cybersecurity and interoperability aviation context, as well as cyberattack monitoring by governments, airports, and airline operators (Klenka 2021).

Hacker types need to be updated to theorize and illustrate their characteristics in the aviation industry

The air transport sector faces the malicious intent of international state and non-state hackers that are willing to exploit innovative technologies such as cloud computing, big data, artificial intelligence (AI), the internet of Things (IoT), machine learning (ML), blockchain techniques, virtual reality (VR), augmented reality (AR), digital twins (DTs), and the metaverse. President Barack Obama emphasized that hackers and cybercriminals are capable of compromising aviation security and sabotage air traffic control systems (Schmidt 2016). In this paper, a hacker is a person who uses bad practices on the Internet to wiretap, spy, alter, sabotage, disrupt, attack, manipulate, interfere, expose, steal, and destabilize a company, country, or critical infrastructure such as an airport or nuclear power plant. Although, hacking is simply the application of computer skills to solve a particular problem. Therefore, we must consider in this manuscript that there are also experts in cybersecurity named "hackers" that contribute to enhancing the country's national security and its critical infrastructure.

Prasad (Prasad 2014) defines a hacker as a person who accesses computers and information stored on computers without obtaining permission. Nevertheless, not all hacking is malicious or illegal, there are experts in cybersecurity who use their hacking skills for ethical practices and protective purposes, such as white, red, blue, green, and nation sponsored hackers (Rawal et al. 2023; Vishnuram et al. 2022). Accessing data on a computer or mobile device without authorization is called hacking. Although hacking a computer to evaluate its security without malicious intent is known as ethical hacking (Vishnuram et al. 2022).

The internet is being used by cybercriminals and insiders as a weapon against airports and commercial airlines (Klenka 2021). The dark web and some video guide tutorials on the internet provide hacking tools without any restrictions, and this should be prohibited for users (Papathanasiou et al. 2023). If we add to this, depending on the type of cyberattack that mutates its signatures and codes to evade detection (called polymorphic attacks) of the Intrusion Detection Systems (IDS), the problems multiply further due to the scalability of cyberattacks in the organization's operating systems. Hackers are continuously changing attack profiles to

breach organizations' security access (Chauhan et al. 2021). As stated by Chng et al. (Chng et al. 2022) there is a need to update our understanding of hacker types and motivations as they evolve. In this study, we identified 12 different typologies of hackers in the aviation context (see Figure 1). We distinguish two types of hackers those who exercise responsibility in proper, effective, ethical, and good practices to improve the safety of citizens and organizations in cities. On the contrary, we also classify those hackers who are developing and using cyberattacks with bad practices to provoke serious material damage to public and private organizations, consumers, or even terrorist acts to kill people.

Then, we analyse hackers that are working to solve cyberthreat and cyberattack incidents:

1. White hacker: She or he is an expert in cybersecurity that examines the vulnerabilities of organizations' operating systems to avoid cyberattacks. Moreover, the white hacker solves and removes the cyberattacks provoked by black hackers and other cybercriminals. For this reason, in this paper, we will call them "White Unicorn" for their enormous safety-security contribution to society. A white hacker helps prevent future cyberattacks and cyberthreats, as well as identify, solve, and remove them (Maalsen 2022). White hackers try to protect data while on the internet with various attacks from hackers and keep it safe with airport and airline operators (Gandhi et al. 2022). Bernardo Quintero (creator of the Virus Total Google company), Tim Berners-Lee, Greg Hoglund, Charlie Miller, Dan Kaminsky, and Jeff Moss are a real example of a white unicorn.
2. Red hacker: She or he is also a certified or authorised person that works for governments. Her main goal is to identify black hackers, cyberterrorists, hacktivists, whistle-blowers, and state-nation hackers, to prevent and eliminate their cyberattacks. Red hackers, who have developed their unique skills by breaking

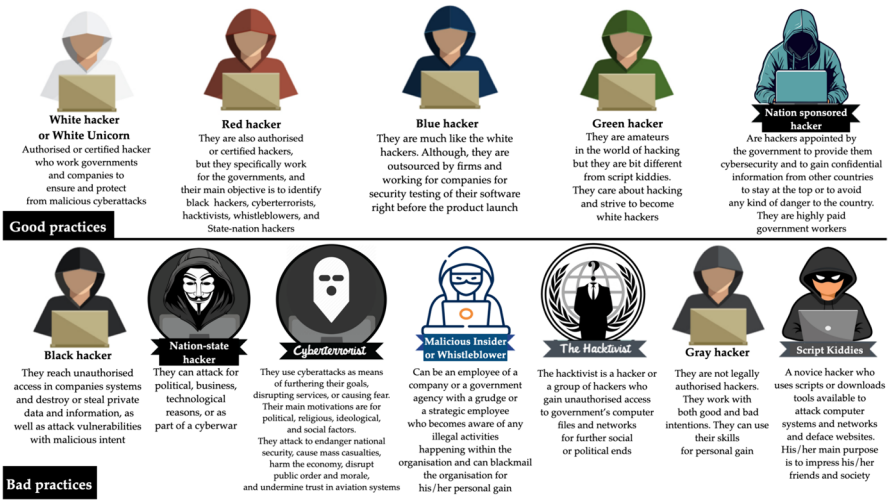

Fig. 1 Types of hackers. Source. The author's own elaboration

into company and government systems, are now being employed for purposes of offensive security against black hackers (Withers et al. 2020).

3. Blue hacker: She or he is a hacker who outsources and works for companies for security testing of their software right before the product launches. Blue hackers also look for loopholes and try to close these gaps (University of Denver 2023).
4. Green hacker: She or he is an amateur in the world of hacking, and their main goal is to be a white, red, or blue hacker. Occasionally, she may not intentionally want to cause harm but may accidentally do so. Green hackers may rely on phishing and other social engineering techniques to bypass security systems (Avast. 2023).
5. Nation sponsored hacker: She or he is a hacker appointed by the government to provide them with cybersecurity and to avoid any kind of danger to the country. This type of hacker is a highly paid government worker, and his or her anonymity must be preserved. Sometimes, these hackers must solve military, cybercrime, and terrorist cyberattacks due to their greater degree of skill and sophistication on the part of nation-states. Moreover, these types of hackers need great economic and technological resources to minimize the likelihood of being discovered (Holt et al. 2023). For instance, the Airbus Group is hit by up to 12 cyberattacks carried out by state-sponsored attackers (Coyne 2016).

Regarding the hackers' bad practices, they are examined because they develop cyberattacks to provoke damage to public and private organizations and the entire society.

6. Black hacker: Also known as Crackers. It is a cybercriminal who illegally cracks systems and destroys or steals private data and information with malicious intent, or even finds software's vulnerabilities to exploit these. Seeking to gain unauthorized access to a computer. In addition, black hackers are highly skilled, and they use their skills in criminal and other activities (Pashel 2007). These cybercriminals are considered by governments to be the most dangerous hackers worldwide, such as Kevin Mitnick, Adrian Lamo, ASTRA, and Tsutomu Shimomura, amongst many others (Kaspersky. 2023b).
7. Nation-state hacker: She or he works for governments, looking to gain access to data or intelligence from other governments or organisations. Moreover, these cybercriminals can attack for political, business, technological, or cyberwar reasons. The results of these attacks can be immense, holding international significance and gaining worldwide media attention. These attackers have greater economic resources to successfully reach their targets (Holt et al. 2023).
8. Cyberterrorist: She or he uses cyberattacks as a means of furthering their goals, disrupting, services, or causing fear. Her or his main motivations are for political, religious, ideological, and social interests. Usually, cyberterrorists are organized groups, such as Al-Qaeda, the pro-Russian NoName057 group, or the Lazarus group. These cybercriminals attack to endanger national security, cause more causalities, harm the economy, disrupt public order and morale, and undermine trust in aviation systems. For instance, the internet is a 'cyberplanning' tool for terrorists and hackers, in fact, terrorists used the internet to plan

their operations and attacks on the US on September 11, 2001 (Timothy 2003; US Department of Justice 2011).

9. Whistleblower: Also known as a malicious insider. An employee of a company who becomes aware of any illegal activities happening within the organization and can blackmail the organization for her or his personal gain. 50% of cybersecurity incidents are caused by insiders, though most are carried out accidentally. In fact, 70% of malicious insider breaches are financially motivated, chiefly through employees selling credentials or access to systems and data on the dark web (Graphus. 2022). Cybersecurity whistleblowing is critical to guarding corporate, public, investor, and consumer safety (Ronickher and LaGarde 2023). One example of this is the case of Edward Snowden in the US. A whistle-blower can alert governments and digital newspapers that a company is grossly negligent. For years, Ed Pierson warned about the safety of the company's 737 Max Jets, saying they were not safe for passengers (Baumgardner 2024).
10. The hacktivist: She or he is a hacker or a group of hackers who gain unauthorised access to the government's computer files and networks for further social, ecological, ethical, or political ends. Today, automated software can do the hacktivist's work without requiring the hacker or /group have great hacking skills (Milan 2013; Romagna 2020). Hacktivism is defined as the use of hacking techniques to promote a political agenda and civil disobedience, as well as gain access to sensitive information and computer networks in an illegal fashion on the Internet (Loh 2023). In 2019, the Ecuadorian embassy in London reported that about 40 million distributed denial of service cyberattacks (DDoS) were directed against the websites and servers of government institutions after the Julian Assange arrest (Paganini 2019).
11. Gray hacker: She or he is not a legally authorised hacker. They work with both good and bad intentions. They can use their skills for personal gain. Gray hackers often look for vulnerabilities in a system without the owner's permission or knowledge. If issues are found, they report them to the owner, sometimes requesting a small fee to fix the problem (Kaspersky. 2023c).
12. Scrip Kiddies: A novice hacker who uses scripts or downloads tools available to attack computer systems and networks and deface websites. Her or his main purpose is to impress her/his friends or society. Script kiddies are generally 14–16 years old and still at school. They tend to be socially maladjusted, preferring to spend their free time working on computers rather than playing with friends (Barber 2001).

All these groups include hackers of varying motivations and skills (Paganini 2019). For this reason, cybersecurity is very important for airport and airline operators because the cyberattacks provoked by cybercriminals must be analysed in different contexts, regions, and motivations to build real progress in cybersecurity knowledge. The challenge of ensuring cybersecurity in air transport is compounded by the volume of air traffic, and cyberattacks will continue to be a critical part of airports and airlines' security agendas (Florido-Benítez 2021; Dave et al. 2022). In 2021, at the Hack in the Box security conference in Amsterdam, Hugo Teso's security consultant demonstrated how easily an airplane could be hijacked remotely using

a simple Android app called PlainSploit (HITBSECCONF2013 Amsterdam 2021). Additionally, cybersecurity researcher Ruben Santamarta found how to hack the satellite communications equipment on passenger jets through their Wi-Fi and inflight entertainment systems (Finkle 2014). After the pandemic crisis, governments, airports, and airline operators need to ensure the safety in of transport with the aim of restoring the tourism and aviation industries (Florido-Benítez 2022).

The main motivations of cybercriminals in the digital world

The ability to protect users and operational systems from both external attacks and insider threats is imperative, and this has become a competitive advantage for airports (e.g., Amsterdam Schiphol, Helsinki-Vantaa, or Miami International airport), and airlines (e.g., Qantas, Emirates, Qatar Airways, or American Airlines). Indeed, the capacity to protect or defend the use of cyberspace from cyberattacks is defined as cybersecurity (Kissel 2011). Cybersecurity is highly related to vulnerabilities, cyberthreats, cyberspace, and cyberattacks, especially in the aviation industry, where technologies play an essential role in monitoring and controlling operations. Lezzi et al. (Lezzi et al. 2018) suggest that most cyberattacks come from companies' software vulnerabilities, information systems, and system security procedures. The risk of a cyberattack is therefore an obvious threat to airports and airlines' safety. The potential that a given threat will exploit the vulnerabilities of a group of assets and cause harm to airport and airline operators is commonly referred to as "risk" (ENISA 2023).

Unfortunately, this study showed some kinds of cyberattacks, and how these are putting passengers and flight crews at risk. Hence, we feel obligated to analyse hackers' motivations, and understand the nature of the cyberattack to make better decisions in an emergency like this. Attribution and identification of hackers cyberattacks is technically complicated in technology, encrypted information, and economic terms. From a researcher's point of view, cyberterrorists' motivations are totally different from gray hackers' purposes. To qualify as a cyberterrorism activity, an attack should result in violence against a person or property, or at least cause enough harm to generate fear.

Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against airports named "critical infrastructures" are considered acts of cyberterrorism (Weimann 2004). We would like to highlight that a cyberattack that damages or destroys an aircraft and persons on board carried out during a period of war, belligerence, or other clash between two states can be considered an act of war (Article 17 of the Chicago Convention) (Abeyratne 2020). In 2014, a Malaysia airlines aircraft was hit by a Russian-made Buk missile over eastern Ukraine, and this missile was fired by Russian-backed separatists. A total of 283 passengers, including 80 children, and 15 crew members were on board (BBC 2020).

Understanding hackers' motivations is key to comprehending the depth of their actions and the damage they can cause. Many hackers take the position that knowing their motivations is the key to understanding their activities hacking is all about

power (McAlaney et al. 2020). For them, the desire to learn and experience challenges motivates their activities. While there are several motivations for hackers, we've covered eight of the most important ones in this paper (see Figure 2).

Hackers' motivations are complex and formed by competing concerns and opportunities such as the attribution of a cyberattack, the enjoyment of the cyberattack from their anonymity and base of operations, monetary gain, and political reward for a cyberattack (Weathersby 2023). Hackers' motivations and cyberattacks can range from the disruption of operational systems to the killing of innocent people. A summary of each motivation type is listed below for better understanding by readers.

- Money: Most hackers are motivated fby economic incentives because they quickly obtain money, and often they cannot be identified by police authorities (Yannakogeorgos 2013). In 2022, hackers stole a record $4 billion in cryptocurrency, led by thieves tied to North Korea (Brooks 2023). A British man stole money from investors' accounts by hacking into email servers and computers belonging to US banks and brokerages, causing more than $5 million in losses. Moreover, a group of hackers stole more than $20 million from the Revolut company in 2023, by exploiting software within its US payment system.
- Financial gain: It is another of the principal motivations of hackers to finance their criminal, military, and illegal activities. Financial gain is one of the most important hackers' motivations because of the monetary reward it brings (Holt 2007). Cyberterrorists and black hackers are the biggest exponents of this illegal motivation. In 2017, hackers infiltrated (data breach) Equifax, and they accessed

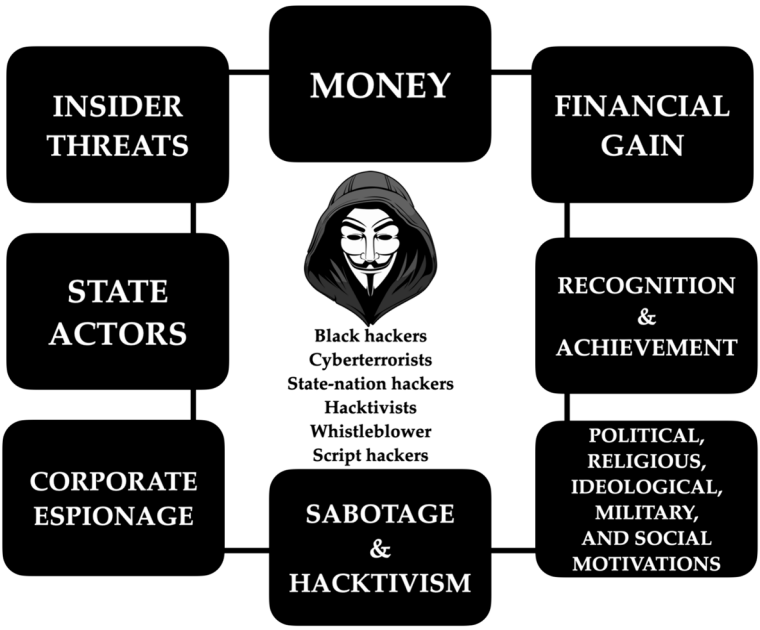

Fig. 2 The main motivations of cybercriminals. Source. The author's own elaboration

the personal information of 147 million individuals. Equifax had to pay $1.4 billion for damage caused (Glen 2023). In 2021, the CNA Financial insurance company paid hackers $40 million after a ransomware attack blocked access to the company's network and stole its data. Hackers seek to steal sensitive information, such as credit card data, personal information, or login credentials, which they can sell on the black market or use for fraudulent activities.

- Recognition and achievement: The thrill of overcoming companies and governments' security measures and infiltrating their systems are other motivations for hackers. The main goal of a pirate is not to be detected. They need to be recognised by other hackers and the international news media that unfortunately disseminate this information. The desire for recognition looms large in the hacking communities. Recognition is earned by its most capable members within this community. This is a powerful motivation for the rest of the hackers because it is only by persevering that they will achieve a higher social status in the hacking community (Hétu et al. 2012). For some, achieving notoriety as a skilled hacker is a powerful incentive. Hackers' psychological needs show their power, revenge, and superiority over others (Cayubit et al. 2017). This motivation also ties into the fact that cybercriminals are very competitive, and they love the challenge their actions bring. Anonymous and Russia's hacking group, Fancy Bear, are the biggest exponents of this type of motivation. In 2022, the hacking group known as Killnet claimed responsibility for knocking on 14 US airport websites.
- Political, religious, ideological, military, and social motivations: Cyberterrorists, hacktivists, and foreign countries are seen as opponents who have this type of motivation and carry out cyberattacks in the name of their cause (Loper 2022; Rogers et al. 2006). Ideological, political, religious, and social motivations inspire hackers to perpetrate and continue cyberattacks around the world (Holt 2009). In addition, Chinese and US hackers frequently engage in cyberattacks against government resources in other nations to obtain sensitive information, map network structures, and military infrastructure (Holt and Kilger 2008). For instance, an Al-Qaeda video called on followers and sympathisers to launch cyberattacks against Western targets (Jayakumar 2020). Hackers are also influenced by their religious, cultural, ideological, and national affiliations. Cyberwar means actions by a nation-state to penetrate another nation's operating systems for the purposes of causing damage or disruption (Jamieson 2020). Cyberwar is currently shaped by new disruptive technologies and the militarization of cyberspace (Pačka and Miroslav Mareš 2023). In 2021, Florido-Benítez (Florido-Benítez 2021) noted that "*future wars and political conflicts will be established in virtual scenarios, where the best soldiers will be elite computer engineers, the best weapons will be complex security systems that disable cyberattacks on terrorism and criminality, and the battlefield will be a strategic digital scenario, where enemies shall not have faces, just a shadow of encrypted codes that governments will have to track and eliminate, that is, a real video game called The Cybernetic Battle*".
- Sabotage and hacktivism: These two motivations are promoted by government agencies, independent organizations, or institutions to disrupt the presidential election in the countries, show the big companies' vulnerabilities, and highlight

human rights. Their main weapons are the spread of misinformation and disinformation, disruption, and the release of sensitive information. In 2022, Russian government bodies and Russia's Federal Security Service were hacked by Anonymous. This group of hacktivists took to Twitter to announce its authorship and request that Russia cease the invasion of Ukraine. Furthermore, the ways in which Russian hacking and social media messaging "propaganda" altered the content of the electoral dialogue and contributed to Donald Trump's victory are examples of sabotage in today's society (Jamieson 2020). Thereby, false and misleading information and its ability to spread rapidly online by hackers and groups of interests have been described as a societal vulnerability and a threat to democracy (Schia and Gjesvik 2020).

- Corporate espionage: This motivation is highly related to intelligence and the use of secret means for strategic ends. Conducted for commercial or financial purposes, corporate espionage involves theft of trade secrets, bribery, blackmail, or surveillance. Cyberespionage is an activity that is practiced all countries and large companies to obtain confidential information and an advantage over a competing organization (Lindsay 2017). For instance, the National Security Agency (NSA) of the US is responsible for information and data for foreign and domestic intelligence and counterintelligence purposes, and this governmental agency cooperates jointly and shares information and data with Google, Apple, Yahoo, Facebook, or Paltack companies for commercial and geopolitical strategic purposes. Most countries spy on other countries to obtain information and then use it as a geopolitical advantage (Lindsay 2017).
- State actors: These hackers are motivated to make cyberattacks because they receive funding and assistance from a nation-state. They are specifically engaged in cybercrime to further their nation's own interests. Typically, they steal information, including intellectual property, personally identifying information, and money. Russia, China, Iran, and North Korea are experts in nation-state attacks, and their main motivations are to attack critical infrastructure and spread of misinformation. Russian state actors used diverse means, from phishing campaigns to zero-days, to gain initial access to devices and networks in industries across the North Atlantic Treaty Organisation (NATO) member states, while malign influence actors sought to intimidate the Ukrainian diaspora and encourage protest movements across Europe (Microsoft. 2023). Stuxnet is one of the most famous nation-state cyberattacks worldwide. While no one officially claimed responsibility for Stuxnet, it is widely accepted that it was a joint creation between the intelligence agencies of the US and Israel (Kaspersky. 2023a). Stuxnet is a powerful computer worm with intelligence that attacked Iranian nuclear systems. It is responsible for causing substantial damage to Iran's nuclear program.
- Insider threats: Insiders' motivations reflect unintentional, ambivalent, or intentional behaviours (Schoenherr 2022). Insiders' motivation can range from stealing data and espionage to criminal intentions or technical challenges. Unfortunately, these actions are devastating for companies because these incidents make it more difficult for IT technicians or experts in cybersecurity to find a threat. Loss of reputation, financial loss, and loss of consumers' confidence in the company are some of the insider's threats (Hunker and Probst 2011). Boeing expe-

rienced one of the longest insider threat attacks in history (1979–2006). An employee stole military manufacturing information from the aerospace company. Nonetheless, the real employer of this actor was Chinese intelligence, which tasked him with acquiring information that would help China improve their space operations (US Department of Justice 2009). Sometimes, hackers hire out third parties that work within a company to carry out the steps of a breach. These malicious insiders provide the hacker with intelligence, access, and other valuable secrets.

As we have seen in hacking motivations, airport and airline operators should be aware of an insider cyberthreat or cyberattack, to know how to detect and respond to the problem. These 8 hackers' motivations emphasise the urgent need for aviation organisations to prioritise cybersecurity measures. E-commerce and critical infrastructure provide massive opportunities for hackers and their planned cyberattacks (Andress and Winterfeld 2013). Hackers seek to compromise operational systems based on ideological beliefs and underlying factors associated with their cause (Holt et al. 2020). To reduce cyberthreats and cyberattacks in the aviation industry, it is advisable to contract security audits performed by experts in cybersecurity that utilize ethical hacking techniques (Holt and Bossler 2008). These services determine where vulnerabilities may be present within operational systems and external services inside the airport.

Cyberattack risks and typologies in the air transport sector

A cyberattack can provoke a chaos in aviation operations because the aviation sector is composed of a lot of service providers. National security agencies do recognise that combating cyberattacks is a shared responsibility in which private organizations and government bodies have an important role to play in the immediate future. Moreover, the use of drones to execute cyber intrusions (e.g., Gatwick, Heathrow, Madrid-Barajas, Frankfurt, Dublin, Saudi Arabia's Abha, and King Abdullah airports) and cyberattacks at airports is a topic of conversation in the air transport sector. Lykou et al. (Lykou et al. 2020) note that airports need to be protected by cyberattacks and drone attacks, known as unmanned aerial systems (UAS), due to an increase in these incidents in the last five years, which is expected to proliferate in frequency, complexity, and severity as drones become larger and more powerful.

Recently, most airports have implemented a security operation centre (SOC) in their infrastructures to monitor and identify cyberthreats and cyberattacks, that is, we are speaking of risk across the entire range of airlines and airports' operational activities that they address throughout the year. A vulnerability is when an operational system is subjected to a natural or external hazard to be exploited by hackers or insiders to cause harm or cyberattacks. Operational systems' vulnerabilities are part of the risk analysis of experts in cybersecurity. Therefore, it is very important to introduce the definition of "risk" in the aviation sector. When there is a probability

that a threat will occur and materialize, causing damage or loss, it is called a risk (Florido-Benítez 2021).

Risk assessment involves monitoring and analysing the safety risks in companies' processes and their operations on a basis. Hazards are classified as large, medium, and low. This test suggests risk management measures and actions. Permanent risk process monitoring by organizations requires preventive safety measures, innovative actions, and the development of contingency plans to tackle future cyberthreats and cyberattacks. Figure 3 illustrates the risk or threat assessment processes in airports and commercial airlines. Airport and airline operators need to constantly evaluate risks and identify ways to mitigate them, as the nature of risks can change over time (Memis 2024). For instance, more than 1,000 applications are running when an Airbus A380 is in the air, thus increasing the likelihood of cyberthreats and risks (Kagalwalla and Churi 2019).

Suppose we consider the risk of a cyberattack on an airport. First of all, it has to be ensured the operability of air traffic control (ATC) and air traffic management (ATM) activities to safeguard the crew and passengers lives in the air, as well as the rest of the workers and passengers at the airport. Then, airport managers should monitor and evaluate the risks and vulnerabilities of aircraft IP networks of flights, airline fleet and route planning systems, cargo handling and shipping, access, departures, and passport control systems, amongst many others, because all of them are

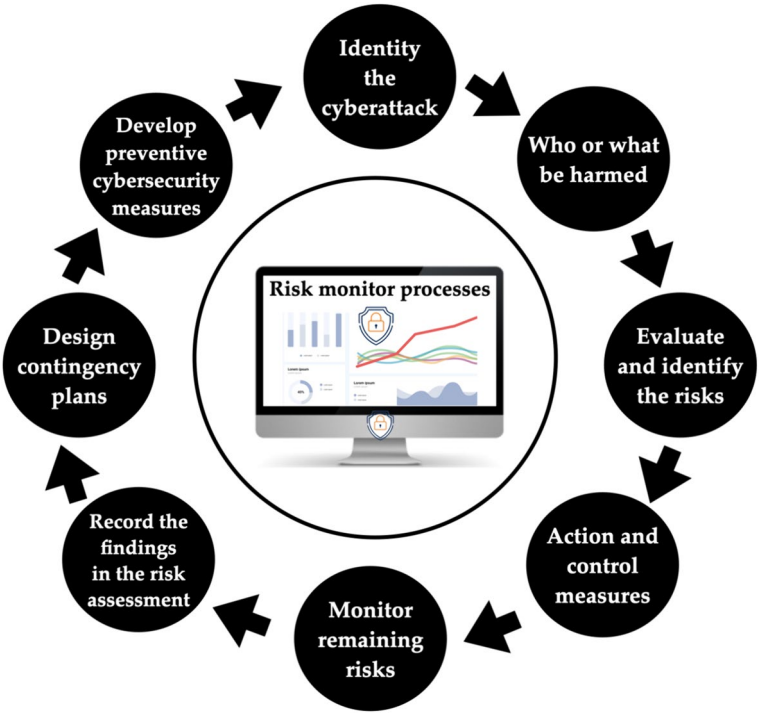

Fig. 3 Risk monitoring processes in airports and commercial airlines. Source. The author's own elaboration

critical to the overall functionality of the airport. The relevance of safety (cyberattack) and hygiene (coronavirus pathogen) protocols has drastically changed the air transport sector to ensure passengers' health and safety (Florido-Benítez 2023c). We must not forget that airports and cargo and commercial airlines provide air accessibility to cities, and the tourism and logistic industries are highly linked to air transport (Florido-Benítez 2023d).

Air transport may have gotten a break from cyberattacks during the COVID-19 pandemic, but cybercriminals are turning their attention to the aviation industry now that travellers are returning to airports. Airport and airline operators can protect themselves by conducting cyber audits, implementing AI monitoring systems, and performing supply chain mapping exercises. Cukier (Cukier 2007) found that 95% of cybersecurity breaches are due to human error, and there is a hacker attack every 39 s in the world. The main types of cyberattacks are set out below and supported by updated studies. Moreover, we would like to point out that, depending on the sector or industry, cyberattacks are different in their typology and frequency. For example, drone denial attacks are more likely to happen near airports than in the e-commerce or health sectors.

- Distributed denial of service cyberattacks (DDoS): This is an attack that blocks the website, operations, or services as a consequence of saturating the server with massive traffic (Teichmann et al. 2023). In 2023, 7 German airports' websites were hit by several DDoS attacks, and these were inoperative, a day after a major IT incident at Lufthansa grounded flights (Hardcastle 2023).
- Drone denial attacks: are attacks perpetrated by drones to intercept communication and control signals, steal data, or even attack airports and airlines, mid-air collisions, and illegal surveillance (Omolara et al. 2023). 70% of experts in the aviation industry are not aware of drone cyberattacks (Omolara et al. 2023). In 2023, three armed drones were shot down over Erbil airport in northern Iraq, where US forces and other international forces are stationed (Al Awsat 2023).
- Hacking: It is the act of exploiting weaknesses in a computer system or network to gain unauthorized access to personal or organizational data (Karpersky. 2023). In 2006, a hacking attack forced the Federal Aviation Administration (FAA) to shut down some of its ATC systems in Alaska, and three years later, another malicious hack accessed the personal data of 48,000 FAA employees (FAA 2009).
- Ransomware: It is an advanced persistent threat that stealthily attacks the information system of an organization operating in the critical sector. This malware tends to encrypt essential files and/or lockout users from the system, bringing the organization's operational activities to a standstill (Mukhopadhyay and Jain 2024). Swissport, the world's largest airport ground services and cargo handling company, was targeted by ransomware hackers in 2022 (Reuters. 2022).
- Phishing: It is a form of deception technique that attackers often use to acquire sensitive information related to individuals and organizations fraudulently (Varshney et al. 2024). In 2013, a phishing attack targeted 75 US airports by an undisclosed nation-state seeking to breach commercial aviation networks (Eurocontrol. 2019).

- Malware: It compromises an organisation sensitive systems and data by infecting them with malicious software (Florido-Benítez 2021). In 2013, the passport control system was locked at Istanbul Atatürk Airport's international departure terminal due to a malware attack (Paganini 2013).
- Slamer worm: It is a computer worm that slows general Internet traffic and crashes routers (Sharma et al. 2023). In 2003, the FAA was hacked by a slammer worm attack, and its administrative server was compromised (Groos 2003).
- Botnets: An attack is the use of automated web requests to defraud, manipulate, and disrupt a website, (Almseidin et al. 2024). Bot attacks use networks of thousands of computers for malicious login attempts or the takedown of a network (Elliot 2019). In 2019, 3 million bot attacks were blocked in a day by Ben Gurion Israel's airport (Solomon 2019).
- Data breaches: These are incidents where unauthorized parties gain access to secured information. A data breach exposes confidential, sensitive, or protected information to an unauthorised person or hacker. Data breaches can occur through a complex set of actions that exploit weaknesses in an airport or commercial airline (Sharma and Barua 2023). In 2023, Scandinavian airline SAS reported that it was hit by a cyberattack and urged customers to refrain from using its app (Mannes 2023).
- Human error: The science of error is merely an aspect of being human. Error is inevitable and can occur even when the best of intentions are set (Connors and Kent 2024). Human factors are the prime weakness that potentially jeopardizes airports, aircraft, and ships' cybersecurity by simply making intentional or unintentional errors, revealing critical information, and generating entry points for hackers and cyberterrorists (Florido-Benítez 2021; Soner et al. 2024). Human error is an employee doing something they should not do. Approximately, 88% of all data breaches are caused by an employee mistake. Human error is still very much the driving force behind an overwhelming majority of cybersecurity problems (Coze 2022; Hancock 2020). In 2017, a contractor doing maintenance work at a British Airways data centre inadvertently switched off the power supply, knocking out the airline's computer systems and leaving 75,000 passengers stranded. The British Airways company cancelled all flights from London's Heathrow and Gatwick airports (Reuters. 2017).
- Crypto-jacking: Tesla's computers were hit by hackers to mine coins; this is known as crypto-jacking (Caporale et al. 2023). It takes place when attackers access someone else's computer to mine crypto currency (Varlioglu, S.: Elsayed, N., ElSayed, Z., Ozer, M. 2022). In 2018, 60% of all computing systems at a European international airport were recently by a crypto jacking (Gatlan 2019).

Cyberattacks perpetrated in the aviation industry from 2000 to January 2024

Regarding the types of cyberattacks in air transport, we will examine the main cyberattacks perpetrated by cybercriminals from 2000 to January 2024, according to KonBriefing (KonBriefing. 2022) and digital newspapers, to stage the reality of

cybersecurity and cyberattacks in the aviation industry context. We selected this period of time because the early 2000s saw the rise of third generation (3G) smartphones with enhanced data services and multimedia capabilities. This year marked the beginning of malware as a mainstream media sensation. In 2000, the ILOVEYOU worm hit Microsoft Outlook users and infected at least 10% of internet-connected hosts in a matter of hours, causing up to $15 billion in damages. It was one of the first cyberattacks documented (SecurityBrief. 2021).

Cyberattacks in the aviation industry increased by 24% worldwide in the first half of 2023 (Surette 2023). We confident that there were more than 54 cyberattacks in the aviation sector (see Fig. 4). In 2020, there were 775 cyberattacks on airlines and 150 at airports (Alohali 2023), but most of them were not published for security reasons. Indeed, most companies, airports, and airline operators do not report cyberattacks to protect their reputation and brand image. In 2019, the British Airways company paid a fine of nearly $230 million for a data breach in 2018, the largest penalty against a company for privacy lapses under the new General Data Protection Regulation (DDPR) law, which allows regulators in each European Union country to issue fines of up to 4% of a company's global revenue for a breach (Satariano 2019). In the case of US and UK countries, companies and individuals are required to report cyberattacks to the US Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the UK's National Cyber Security Centre respectively. In 2016, only 28% of cyberattacks against businesses in the UK were reported to the police (Swinhoe 2019).

Figure 4 shows 54 cyberattacks documented and analysed in this research. Of the total cyberattacks in the period analysed, 35 were perpetrated at airports (65%) and

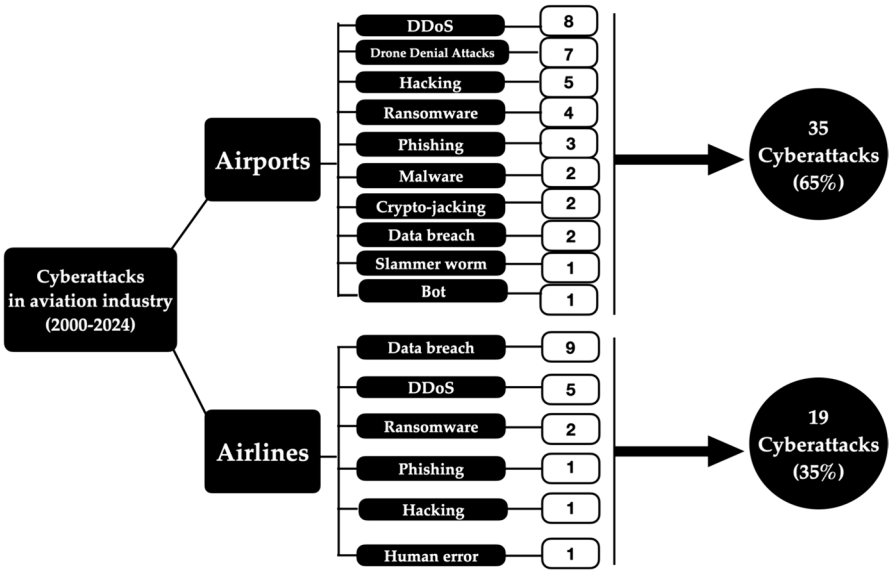

Fig. 4 Cyberattacks perpetrated in aviation industry from 2000 to January 2024. Source. Author's own elaboration from KonBriefing (KonBriefing. 2022) and digital newspapers

19 by airlines (35%). Regarding airports, the most common types of cyberattacks have been DDoS with 8 incidents, followed by drone denial-of-service attacks with 7, hacking with 5, ransomware with 4, phishing with 3, malware, data breach, and crypto-jacking with 2, respectively, and bot and slammer worm with 1, respectively. DDoS attacks target to airports' websites and apps to steal private information and sensible data. What compounds the problem is that cybercriminals share their findings on the dark web with the hacker community and sell this information for large sums of money. Indeed, DDoS is one of the most common attacks in the aviation industry because it renders the network useless by overloading the channel with meaningless messages to steal data (Lewis 2019). Commercial airlines also suffered multiple DDoS attacks (5) during the established period of this research, and it must be considered a serious vulnerability and threat for airline operators. For this reason, cybersecurity must be a priority and not a necessity in the aviation industry. Safety is the most important factor in air transport for both passengers and companies.

Most airports are vulnerable to DDoS attacks due to the broadcast nature of wireless communication (Bicakci and Tavli 2009). One of the most difficult tasks of protecting an airport is to analyse and detect who organisations, countries, or people are willing to attack this critical infrastructure and airlines. For instance, the FAA continues to use outdated systems, some of which are 30 years old. These systems could be vulnerable to cyberattacks, especially from hackers backed by adversarial nations (Surette 2023). Such an attack could have catastrophic consequences for the US, given its reliance on air travel (Surette 2023).

Concerning drone denial-of-service attacks, we must be aware that drones can collect confidential data, weapons, drugs, and transport explosives, chemical bombs, drugs, various types of jammers, amongst many others. Hence, hackers and cyberterrorists can use this emerging technology to inflict mass injuries and life sacrifices. We found that 7 drone attacks have been perpetrated against airports and airlines, respectively. Edinburgh, Madrid, Palm Beach, Warsaw, Pittsburgh, and Frankfurt airports suffered serious drone incidents in 2023, causing flight cancellations, delays, high economic losses for airport and airline operators, and bad experiences for passengers. The drone attack that disrupted Gatwick airport (UK) for three days in 2019 cost the airport £1.4 million, and the EasyJet operator reported that the attack cost it £15 million in compensation and welfare payments to passengers, as well as lost revenue (Topham 2019). Worse still was a terrorist attack with 13 armed drones and a global positioning system (GPS) that attacked 4 Russian bases in Syria. Each drone had half a kilogram of explosives, and these were launched from a site more than 31 miles (50 kms) distant from their target. This extremely serious attack occurred in 2018 (Brown 2018).

As airports increasingly use digital technology in their day-to-day operations, they are becoming more vulnerable to data breaches. Although this study has accounted for 2 data breaches in airports and 9 in commercial airlines, we cannot afford to underestimate hackers to unauthorized access to secured information and airport' and airline control systems. Airports and airlines are very attractive to cybercriminals in search of personal information and data because both of these sectors are custodians of vast amounts of sensitive data. In 2020, San Francisco airport (US) revealed a data breach on its two official websites through an employee

credential, endangering the airport's safety and that of its workers (Bîzgă 2020). A data breach provides a plethora of information and privilege escalation to hackers, offering them the ability to move around the airlines and airports' operational systems at will. Airport operators are concerned about IoT technologies inside the airport's terminal because they can be used for malicious purposes or data breaches (Lykou et al. 2018a). Airline data breaches are becoming increasingly commonplace, but this has negative effects on their profits and brand image. Its shares, which are listed on the Hong Kong Stock Exchange, fell by 3.8% of their market value ($201 million) when the details of the data breach were published on TV and in digital newspapers (Meyer 2018). Findings reveal that data breach incidents provoke grave economic and social consequences for consumers and airport and commercial airline operators, not to mention, that a terrorist attack can occur through a vulnerability (data breach) in an aircraft's control systems and kill hundreds of passengers.

Moreover, these findings suggest that airports and airlines are constantly exposed to vulnerabilities and cyberattacks, and they have to improve the cybersecurity in their operational systems. For instance, airlines and airports' applications and websites are very relevant to provide information and contents to passengers, as well as a sales and marketing tool to increase revenues and new customers (Florido-Benítez and Alcázar 2015; Florido-Benítez 2016). Nevertheless, a study carried out by Sukesh et al. (Sukesh et al. 2023) found a rise in data breaches in the Air India airline and how these vulnerabilities could be used by hackers to attack the airline and steal customers' personal information. From 1960 to 2000, the aviation system was not prepared for cyberattacks (Leśnikowski 2021). In 2008, some of the Boeing 787 Dreamliner's products and services were removed and required by the FAA due to possible vulnerabilities that could create a threat to the aircraft (Magazine 2008; FAA 2008). According to the Department for Science, Innovation, and Technology of the UK, data breaches cost each UK business, of any size, an average of approximately £1,100, for medium and large businesses £4,960, and for charities £530 (Department for Science 2023).

Among the numerous cyberattacks faced by the aviation industry, 4 and 2 ransomware attacks were suffered by airports and airlines, respectively, over the period considered. This number likely underestimates the actual occurrence. Indeed, Bridewell, a cybersecurity company, reported an alarming rise in airports and airlines' ransomware attacks in 2023, and many more were not reported because no company wants to admit when they've had these cyberattacks (Reed 2023). A ransomware attack can paralyze an airport's daily operations, impeding access to essential operational technology such as baggage handling (BHS), building management systems (BMS), flight management (FMS), and supervisory control and data acquisition (SCADA) systems. Thus, airport and airline operators need to include a cybersecurity culture among their employees, invest in cybersecurity tools, and recruit experts in cybersecurity to ensure proactive defence against sophisticated polymorphic attacks.

Sabeel et al. (Sabeel et al. 2023) note that methods based on machine learning (ML), deep learning (DL), blockchain, and AI techniques help to detect and mitigate ransomware and polymorphic attacks. In 2018, the Bristol airport was hacked by a ransomware, causing flight display screens to fail for two days. Hackers demanded

payment (cryptocurrency) to unencrypt the lost data. The Bristol airport operator refused to pay it and took the infected systems offline to manually restore them (The hacker News 2018). The airport operator's decision to pay the ransom often becomes a complex matter, influenced by the possible impact on both airport operations and passenger safety. Figure 5 illustrates the main risks of paying a ransom in the aviation industry: information and data loss, loss of trust by customers and partners, contravention of insurances companies' policies and their recommendations, possible criminal liabilities and penalties by the justice system, increased vulnerability for future cyberattacks by hackers, and reinforcement and funding of criminal activities.

Sometimes, there is no guarantee that hackers will return operators stolen data or information for the payment made; that is, airport and airline operators ought to reflect on the risks of making cyberattack payments. In 2020, half of the US firms that actually paid ransoms were unable to recover all their data, and of the total US companies that suffered a ransomware attack, 68% paid the ransom (HYCU 2023). These results suggest that paying the ransom also puts airports and airlines at increased risk for a cyberattack in the future and encourages other cybercriminals to repeat the same cyberattack. Leading insurer Lloyd's of London reported a dire warning about a potential cyberattack scenario on one of the world's major payment systems, estimating that the global cost would total about $3.5 trillion and that much of the recovery cost would not be covered by insurance policies (Smith 2023).

Hacking is also another common incident in airports and airlines, 5 hacking attacks were accounted for in airports and 1 in commercial airlines in this study. In 2023, Long Beach airport located near Los Angeles, California, was the target of a hacking attack. The cyberattack affected the airport's main website and caused

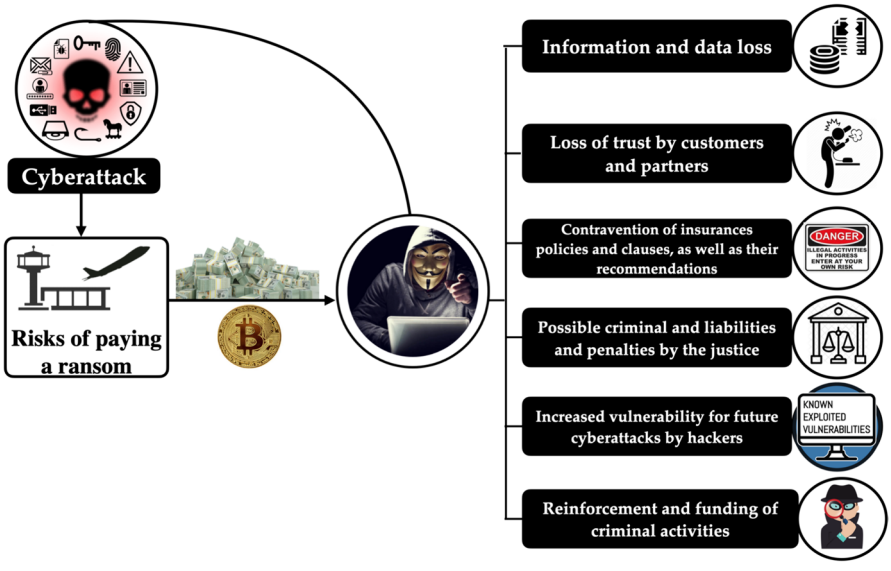

Fig. 5 The main risks of paying a ransom in the aviation industry. Source. Author's own elaboration

the airport authority to take the website offline temporarily, provoking some of the payment processing systems that were linked to the website (Homeland Security Today 2023). Many hackers consider hacking attacks an easy, cheap, and very effective means of demonstrating their strength. Hackers find vulnerabilities in aircraft control systems, and they can jeopardize the safety of both crews and passengers. When it comes to aircraft and Wi-Fi connections, mitigating risks is crucial to guaranteeing physical security (Faruk et al. 2021). In 2011, hackers were able to gain access to the radio frequencies used by British air traffic controllers, and they gave false information to the pilots and sent a false signal about the danger (Żmigrodzka 2020). Findings suggest that there is a lack of education and understanding in cybersecurity. Therefore, enhancing awareness of cybersecurity and cyberattacks effects on air transport is very important to address future and possible cyber incidents. In this study, we recommend that all pilots undergo cybersecurity training and a cyberattack drill annually to ensure that they can recover when computers fail on-flight. This training will help them to know whether the signals are trustworthy in the aircraft's control systems or whether the system was attacked.

Taking into account the spectrum of the variety of possible attacks, it is necessary to describe a given phenomenon in more detail, a phishing attack. 3 and 1 phishing incidents were perpetrated in airports and airlines, respectively. This type of attack has increased during and after the COVID-19 pandemic, particularly in airports, stealing sensible information and data, money, and causing operational disruptions (ElMarady and Rahouma 2022; Singh and Loura 2022). The EATM-CERT agency (European Air Traffic Management Computer Emergency Response Team) detected that 15,493 accounts of 30 airlines were offered for sale on the dark web, worth over 400 thousand euros, possibly all of these data were stolen through phishing and data breach attacks (Eurocontrol. 2023). In 2019, the personal data of over 120,000 customers was compromised following a phishing attack after accessing Air New Zealand's (Phillips et al. 2022).

The rest of the cyberattacks accounted for in this manuscript, such as malware, crypto-jacking, slammer worms, botnets, or human error, had a minor impact on airports and airlines but were not less significant in terms of safety and threat. More than 88% of all general aviation accidents are attributed to human error (Wilson Kehoe Winingham Team 2022). For instance, possibly a human error caused a recent collision between a Japan Airlines jetliner and a Japan Coast Guard (JCG) plane at Haneda airport on January 2024, due to the communication records show that the JCG aircraft was not given permission to take off, and the aircraft proceeded onto the runway without staying on the taxiway (Shimbun 2024).

To conclude this section, we would like to stress that the spectrum of cyberattacks analysed in this research shows that airport and airline operators must implement effective cybersecurity protocols and systems to mitigate cyber incidents. In addition, there are still too many vulnerabilities in the aviation industry, as evidenced in this study, particularly in relation to airports' operational activities and aircraft's flight control software. It is imperative for the aviation industry to mitigate risks and protect their operational systems and sensitive data from cyberattacks. This is known as cyber resilience, which is defined as the ability to predict, detect, respond, and recover from cyberattacks and cyberthreats. Learning from cyberattacks is

crucial for airport and airline operators to improve their cyber resilience and effectively respond to evolving threats (Patterson et al. 2024).

Practical and theoretical implications, limitations, and future research

The sustainability of airports and airlines' operations is highly dependent on cybersecurity protocols as a preventive tool to ensure the security of business-to-consumer (B2C) and business-to-business (B2B) electronic transactions. For instance, the implementation of digital twins' tools at organizations is currently used in cybersecurity to reduce cyberthreats and cyberattacks. Undoubtedly, the functioning of the aviation industry is based on public trust, which can be irreversibly undermined by the cyberattack incidents that we previously mentioned. Each airport and airline should have their own cybersecurity programs, protocols and supported by good governance by regional and national governments. It is essential to have a global vision that addresses all threats to air transport, not just cyberattacks in airports. The interoperability between airport operators and governments boosts better recommend solutions to cybersecurity incidents (Florido-Benítez 2021). Airports are the main gateway to the world for travellers and business; thus, they are of great importance for country development and economic growth (Florido-Benítez 2020).

Recently, both EASA and FAA organizations have created regulations to tackle cyberattack incidents in the air transport sector. Conversely, aviation sector firms are pushing back on efforts by the Transportation Security Administration (TSA) to mandate that all cybersecurity incidents are reported to the Cybersecurity and Infrastructure Security Agency (CISA) within 24 h (Greig 2022). Therefore, greater efforts are required to create and align a common framework for an international cybersecurity recommendation in the aviation industry, as well as report all the cyberthreats and cyberattacks to the CISA organization. Technical cybersecurity protocols help to enhance airlines and airports' cyber defence and resilience (Lykou et al. 2018b). To ensure and guarantee the security of data and private information in B2B and B2C in the aviation industry, we recommend the following lines of action to prevent cyberattacks, which are shown in Fig. 6.

The implementation of cybersecurity tools, protocols, and systems must be a priority for the aviation industry and their stakeholders or partners. For instance, identifying possible cyberthreats and motivations by cybercriminals helps develop proactive cybersecurity measures to combat cyberattacks. Another relevant action that should be included in the implementation of cybersecurity systems is that airport and airline operators require highly qualified IT technicians and experts in cybersecurity to analyse/monitor/solve/eliminate possible cyberthreats and cyberattacks, as well as develop contingency plans to coordinate and minimize future cyber incidents. The integrity and security of information and data have become much more vulnerable in the aviation industry as a result of airports and airlines are more digitalised and connected between them and passengers. According to the International Civil Aviation Organization (ICAO) (ICAO 2022) notes that new cybersecurity

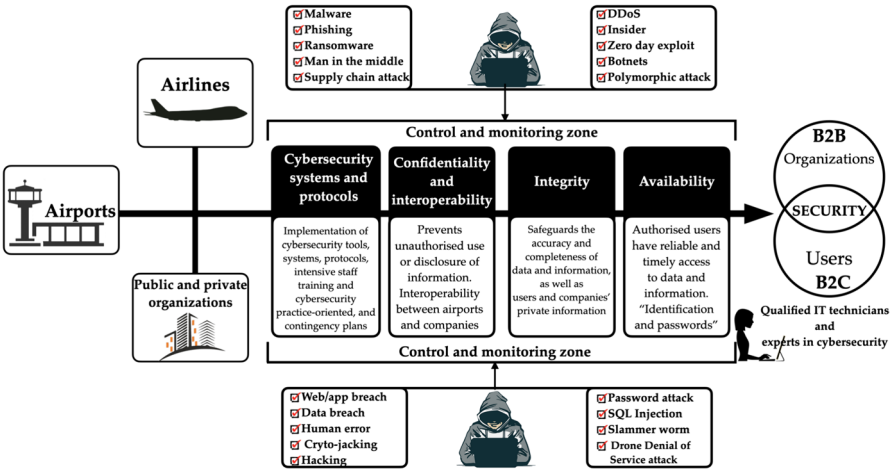

Fig. 6 Ensure and guarantee the security of data and private information for B2B and B2C in the aviation industry. Source. The author's own elaboration

protocols and innovative safety initiatives and debates will increase the aviation sector's resilience.

Confidentiality and interoperability are crucial factors to ensure the security of operational activities and their transactions in information and data terms at airports, airlines, and the rest of the companies that converge in the aviation sector. Organizations need to prevent the unauthorised and illegal use or disclosure of information. Therefore, interoperability among airports, airlines, and partners enhances operational procedures that have a direct impact in the short and medium term on cybersecurity and protection of confidential information and data, especially in B2B and B2C activities and transactions. Confidentiality's information and data in aviation refer to how much personal information should be made available to your organization and who has access to it. To enable information and data scalability according to employees' responsibilities. A maintenance worker cannot access the same information as an expert in airport of cybersecurity, it would be unthinkable and counterproductive to prevent cyberthreats. For instance, blockchain technology monitors the traceability of information to protect databases. A cybersecurity culture in organizations improves employees' overall safety performance and users' personal information in airports (Hagos et al. 2023). Organizations must assess if there are any deficiencies in their operational activities (Mooren and Grzebieta 2010). Airport and airline operators must ensure the communication and messages exchanged through the network are generated by legitimate nodes and cannot be modified or suppressed by a hacker (Niraula 2022).

Information integrity becomes increasingly critical as automated systems become less reliant on human oversight and their ability to ensure information is suitable for its intended use. In air cargo and logistic activities, data integrity plays a vital role in ensuring the quality of logistics services. Data protection and privacy are two major concerns in logistics, and organizations have implemented

blockchain and encryption schemes to provide tamper-proof authentication services and verification of transactions in cash logistics processes in their processes (Albshaier et al. 2024). The accuracy and completeness of data and information require the safeguarding of organizations as well as users and companies' private information. A key process for managing quality management systems in the aviation industry is to ensure data and information integrity (Cheung et al. 2021). Karamitsos et al. (Karamitsos et al. 2023) suggest that blockchain technology secures employee authentication processes, confidential data, and information tracking, monitors employee identities, and eliminates vulnerabilities and cyberattacks.

Concerning the availability of information and data at organizations, authorised users have reliable and timely access to data information through the user's identification and password. For instance, the FlighRadar24 platform provides data and information about airport delays to users and passengers, however, Hugo Teso's security consultant hacked an aircraft's control systems through an application (HITBSECCONF2013 Amsterdam 2021; Artamonov et al. 2022). In 2016, approximately 300 passes for Sodexo Catering employees at Heathrow airport were suspended on suspicion of fraudulent activities (Al-Othman 2016). Obviously, airport and airline operators' information and data availability can have negative safety and commercial consequences if not properly planned and managed. Sometimes, communicating and providing detailed information about operational activities to workers and users can put at risk the airport's own commercial activity and the safety of passengers.

Furthermore, this manuscript provides theoretical implications for academics and researchers seeking to know hackers' characteristics, motivations, and consequences in society. This study also included a new literature review of hackers and their typologies, motivations, and types of cyberattacks, as well as cyberattacks perpetrated in the aviation industry from 2000 to January 2024, to help researchers and airport and airline operators make better decisions against future cyberthreats and cyberattacks. Indeed, this research illustrates the crude reality of cyber incidents in the aviation industry, and how cyberattacks have multiplied in the last few years. 530% of the cyberattacks increased in European aviation in 2020 (Eurocontrol. 2021).

The increasing attention given to the dangers of cyberattacks is on the rise, but unfortunately, the majority of airport and airline operators are not well equipped to address the issue. As researchers, we must develop new future research that helps the aviation industry mitigate cyberattacks and their horrible consequences. Addressing airports' new cybersecurity challenges not only prevents disruptions and improves the safety of passengers and workers, but also improves their competitive advantage and brand image. Additionally, we detected that there are limited studies related to cybersecurity and cyberattack topics related to the air freight and logistics sectors, thus, further research is necessary to explore cyberattack impacts in the air cargo and logistics industries. In addition, we argue that 54 cyberattacks perpetrated in the aviation industry as a result of airlines and airports' vulnerabilities should be included in a database accessible to researchers, airline and airport operators, and government bodies.

Based on our findings, this study encourages the improvement of the quality of information and data on cyberattacks by national governments and the aviation industry. To seek information and data about hackers' motivations and types of cyberattacks in digital newspapers is very complicated because most organizations do not report cyberattacks to protect their reputation and brand image; in fact, this has been one of the main limitations of this manuscript. Moreover, airport and airline operators did not provide specific and real information about cyberattacks that occurred in their operations and commercial activities. This makes it difficult to detect true hackers' motivations and how they have planned and developed the cyberattacks. One in five UK businesses (20%) admit to not being confident in knowing what to do should a cyberattack happen, and far less to report it to the police for fear of the financial and legal repercussions (AVIVA 2023). Future research could focus on the number of companies, airlines, and airports that have been penalised by the justice system and have paid a fine because they did not report a cyberattack to the DDPR agency and other governmental organizations. To conclude this section, this research offers noteworthy practical and theoretical implications for organizations, and researchers seek to boost cybersecurity in the aviation industry to combat future cyberattacks. Air transport is highly exposed to cyberattacks by hackers to gain money and cause serious property damage or mortals (Civil Aviation Authority 2023; Florido-Benítez 2024).

Conclusions

The main objective of this study was to analyse the types of hackers and cyberattacks in the aviation industry to enhance cybersecurity in the air sector. This research has identified 12 different typologies of hackers in the aviation context. First, those hackers who exercise responsibility in proper, effective, ethical, and good practices to improve the safety of citizens and organizations, such as a white unicorn, red, blue, green, and nation sponsored hackers. And second, those hackers that are developing and using cyberattacks with bad practices to provoke serious material damage to public and private organizations, consumers, or even terrorist acts to kill people, including black, nation-state, cyberterrorist, whistle-blower, hacktivist, script kiddie, and gray hackers. Furthermore, findings reveal 54 cyberattacks documented in the period analysed (2000 – January 2024).

Of the total cyberattacks in the period analysed 35 were perpetrated at airports (65%) and 19 ny airlines (35%). 8 and 5 DDoS attacks have been perpetrated in airports and airlines, respectively, DDoS attacks have become the most common attacks in the aviation industry because this type of attack does not require great resources and knowledge to carry out. Airports and airlines are vulnerable to DDos attacks because they both use digital technology and wireless communication in their day-to-day operations. For this reason, cybersecurity must be a priority and not a necessity in the aviation industry. Safety is the most important factor in air transport for both passengers and companies.

We would like to provide the main motivations of hackers in these 54 incidents that occurred in the aviation industry, but it is really impossible to know because

most cyberattacks are usually carried out by cybercriminal anonymous, which can't be traced. In addition, airport and airline operators and digital newspapers are reluctant to provide detailed information on the facts related to hackers and their motivations. Possibly, it is because organizations are engaged in a process of investigation and cooperation with police authorities, or even a negotiation with hackers to pay a ransom to recover the stolen information and data, as we have seen previously.

Another finding was that data breach incidents provoke grave economic and social consequences for consumers and airport and commercial airline operators, not to mention, that a terrorist attack can occur through a vulnerability (data breach) in an aircraft's control systems and kill hundreds of passengers. Indeed, each cyberattack has its own actor, codes, strategy, typology, motivation, impact, and solution. For instance, it is not the same as exploiting a vulnerability in aircraft flight control software to commit a terrorist act that a cyberattack makes necessary to close the visits in the Toronto Zoo in Canada.

Therefore, the air transport industry faces increased cyberthreats and cyberattacks due to hyperconnectivity and the lack of standardized frameworks and cybersecurity defences. Moreover, enhancing awareness of cybersecurity and cyberattacks effects air transport is very important to address future and possible cyber incidents. We recommend that all pilots undergo cybersecurity training and a cyberattack drill annually to ensure that they can recover when computers fail on-flight. This training will help them to know whether the signals are trustworthy in the aircraft's control systems or whether the system was attacked.

Acknowledgements The author would like to thank anonymous reviewers and editors for providing valuable suggestions and comments.

Author contributions Conceptualization, L.F.-B. methodology, L.F.-B.; validation, L.F.-B.; formal analysis, L.F.-B.; investigation, L.F.-B.; resources, L.F.-B.; data curation, L.F.-B.; writing—original draft preparation, L.F.-B.; writing—review and editing, L.F.-B.; visualization, L.F.-B.

Funding Funding for open access charge: Universidad de Málaga / CBUA. The author would like to thank anomymous reviewers and editors for providing valuable suggestions and comments, as well as the University of Malaga.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

References

Abeyratne R (2020) Aviation and cybersecurity in the digital world. In: Aviation in the Digital Age. Springer, Cham, pp 173–211. https://doi.org/10.1007/978-3-030-48218-3_10

ACI (2021) Airport cybersecurity in a COVID-19 world. Available at: https://blog.aci.aero/airport-cybersecurity-in-a-covid-19-world/. Accessed 1 Jan 2024

Adenigbo AJ, Mageto J, Luke R (2023) Adopting technological innovations in the air cargo logistics industry in South Africa. Logistics 7:84. https://doi.org/10.3390/logistics7040084

Ahsan M, Nygard KE, Gomes R, Chowdhury MM, Rifat N, Connolly JF (2022) Cybersecurity threats, and their mitigation approaches using machine learning—a review. J Cybersecur Priv 2:527–555. https://doi.org/10.3390/jcp2030027

Airbus (2020) 5 actions to protect your aircraft from cyberattacks. Available at: https://aircraft.airbus.com/en/5-actions-to-protect-your-aircraft-from-cyberattacks. Accessed 6 Jan 2024

Al Awsat A (2023) Armed drones shot down over Northern Iraqi airport where US forces are based. Available at: https://english.aawsat.com/arab-world/4653341-armed-drones-shot-down-over-northern-iraqi-airport-where-us-forces-are-based. Accessed 3 Jan 2024

Albshaier L, Almarri S, Hafizur Rahman MM (2024) A review of blockchain's role in e-commerce transactions: open challenges, and future research directions. Computers 13:27. https://doi.org/10.3390/computers13010027

Almseidin M, Al-Sawwa J, Alkasassbeh M, Alzubi M, Airfou KDT-ARO (2024) Decision tree-based artificial rabbits optimization to mitigate IoT botnet exploitation. J Netw Syst Ma 32:14. https://doi.org/10.1007/s10922-023-09785-6

Alohali BA (2023) Aviation cybersecurity national governance. Available at: https://www.icao.int/MID/Documents/2023/Cybersecurity%20Symposium/2.2%20Saudi%20Arabia%20-%20Aviation%20Cybersecurity%20National%20Governance.pdf. Accessed 3 Jan 2024

Al-Othman H (2016) 300 Heathrow staff have passes suspended amid security scam probe. Available online: https://www.standard.co.uk/news/crime/investigation-launched-into-security-pass-scam-at-heathrow-airport-a3317371.html. Accessed 24 Jan 2024

Andress J, Winterfeld S (2013) Cyber warfare: techniques, tactics and tools for security practitioners. Elsevier, USA

Artamonov I, Danilochkina N, Pocebneva I, Karmokova K (2022) Using data integrity models for aviation industry business process quality management. Tra Re pro 63:1668–1673. https://doi.org/10.1016/j.trpro.2022.06.180

Avast (2023) Hacker types: black hat, white hat, and gray hat hackers. Available at: https://www.avast.com/c-hacker-types#:~:text=Green%20hat%20hackers%20are%20"green,but%20may%20accidentally%20do%20so. Accessed 14 Jan 2024

AVIVA (2023) One in five businesses have been victims of cyberattack in the last year. Available at: https://www.aviva.com/newsroom/news-releases/2023/12/One-in-five-businesses-have-been-victims-of-cyber-attack-in-the-last-year/. Accessed 25 Jan 2024

Barber R (2001) Hackers profiled—who are they and what are their motivations? Co Fra Se 2:14–17. https://doi.org/10.1016/S1361-3723(01)02017-6

Baumgardner G (2024) Boeing whistleblower 'not at all' surprised after door plug blows of MAX 9 midflight. Available at: https://www.kiro7.com/news/local/boeing-whistleblower-not-all-surprised-after-door-plug-blows-max-9-midflight/AR75VNCXKRDPFN3MKEBHU3OIEA/. Accessed 12 Jan 2024

BBC (2020) MH17 Ukraine plane crash: What we know. Available at: https://www.bbc.com/news/world-europe-28357880. Accessed 17 Jan 2024

Bicakci K, Tavli B (2009) Denial-of-Service attacks and countermeasures in IEEE 802.11 wireless networks. Co Sta Int 31:31–941. https://doi.org/10.1016/j.csi.2008.09.038

Biju JM, Gopal N, Prakash AJ (2019) Cyberattacks and its different types. Int Re J En Te 6:4849–4852

Bîzgă A (2020) San Francisco international airport reveals data breach on two websites. Available at; https://www.bitdefender.com/blog/hotforsecurity/san-francisco-international-airport-reveals-data-breach-on-two-websites/. Accessed 18 Jan 2024

Brooks KJ (2023) Hackers stole record $4 billion in cryptocurrency last year. Available at: https://www.cbsnews.com/news/cryptocurrency-hackers-stole-3-8-billion-north-korea-chainalysis-report/. Accessed 17 Jan 2024

Brown D (2018) Russia's explanation about who attacked its bases in Syria keeps getting stranger. Available at: https://www.businessinsider.com/russia-strange-explanation-drone-attack-syria-bases-us-turkey-2018-1. Accessed 17 Jan 2024

Buchanan B (2020) The hacker and the state: Cyberattack and the new normal of geopolitics. Harvard University Press

Caporale GM, Kang WY, Spagnolo F, Spagnolo N (2023) Cyberattacks, cryptocurrencies and cyber security. In: Achim, M.V. (eds) Economic and Financial Crime, Sustainability and Good Governance. Contributions to Finance and Accounting. Springer, Cham. https://doi.org/10.1007/978-3-031-34082-6_14

Cayubit RFO, Rebolledo KM, Kintanar RGA, Pastores AG, Santiago AJA, Valles PB (2017) A cyber phenomenon: a q-analysis on the motivation of computer hackers. Psychol Stud 62:386–394. https://doi.org/10.1007/s12646-017-0423-9

Chauhan R, Sabeel U, Izaddoost A, Shah Heydari S (2021) Polymorphic adversarial cyberattacks using WGAN. J Cybersecur Priv 1:767–792. https://doi.org/10.3390/jcp1040037

Cheung KF, Bell MG, Bhattacharjya J (2021) Cybersecurity in logistics and supply chain management: An overview and future research directions. Tra Re E Lo Tra Re 146:102217. https://doi.org/10.1016/j.tre.2020.102217

Chng S, Lu HY, Kumar A, Yau D (2022) Hacker types, motivations, and strategies: A comprehensive framework. Co Hu Be Re 5:100167. https://doi.org/10.1016/j.chbr.2022.100167

Civil Aviation Authority (2023) Aviation industry's battle with cyberattacks. Available at: https://caa.gov.qa/en/news/aviation-industrys-battle-cyber-attacks. Accessed 25 Jan 2024

Connors C, Kent PS (2024) The science of human error. In Handbook of Perioperative and Procedural Patient Safety. Elsevier pp 1–8. https://doi.org/10.1016/B978-0-323-66179-9.00014-2

Coyne A (2016) How Airbus defends against 12 big cyberattacks each year. Available at: https://www.itnews.com.au/news/how-airbus-defends-against-12-big-cyber-attacks-each-year-418131. Accessed 13 Jan 2024

Cukier M (2007) Study: hackers attack every 39 seconds. Available at: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds. Accessed 17 Jan 2024

Dave G, Choudhary G, Sihag V, You I, Choo KKR (2022) Cybersecurity challenges in aviation communication, navigation, and surveillance. Co Se 112:102516. https://doi.org/10.1016/j.cose.2021.102516

Department for Science, Innovation, and Technology (2023) Official statistics cyber security breaches survey 2023. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023. Accessed 20 Jan 2024

EASA (2021) Cybersecurity overview. Available at: https://www.easa.europa.eu/domains/cyber-security/overview. Accessed 4 Jan 2024

Elliot C (2019) Hackers are targeting airlines in record numbers. Here's what that means for you. Available at: https://www.forbes.com/sites/christopherelliott/2019/02/25/hackers-are-targeting-airlines-in-record-numbers-heres-what-that-means-for-you/. Accessed 11 Jan 2024

El-Maissi AM, Kassem MM, Nazri FM (2023) Resilient Critical Infrastructures: an Innovative Methodological Perspective for Critical Infrastructure (CI) integrated assessment models by inducing digital technologies during multi-hazard incidents. MethodsX 9:102561. https://doi.org/10.1016/j.mex.2024.102561

ElMarady, A.A.; Rahouma, K.H. (2022). The Impact of COVID-19 on the Cybersecurity in Civil Aviation: Review and Analysis. In 2022 International Telecommunications Conference (ITC-Egypt). IEEE. 1–6. https://doi.org/10.1109/ITC-Egypt55520.2022.9855692

ENISA (2023) Glossary. Available at: https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary. Accessed 10 Jan 2024

Eurocontrol (2019) ATM cyber security awareness workshop. Available at: https://www.icao.int/Meetings/AVSEC2019/Documents/Air%20Traffic%20Management%20Cyber%20Security%20Awareness%20_Part_I.pdf. Accessed 7 Jan 2024

Eurocontrol (2021) Aviation under attack from a wave of cybercrime. Available at: https://www.eurocontrol.int/publication/eurocontrol-think-paper-12-aviation-under-attack-wave-cybercrime. Accessed 1 Jan 2024

Eurocontrol (2023) European air traffic management computer emergency response team. Available at: https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team. Accessed 21 Jan 2024

European Parliament (2021) The future of regional airports: challenges and opportunities. Available online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/689346/EPRS_BRI(2021)689346_EN.pdf. Accessed 7 Jan 2024

FAA (2008) Providing the safest, most efficient aerospace system in the world. Available at: https://www.faa.gov. Accessed 20 Jan 2024

FAA (2009) Review of web applications security and intrusion detection in air traffic control systems. Available at: https://www.oig.dot.gov/sites/default/files/ATC_Web_Report.pdf. Accessed 2 Jan 2024

Faruk MJH, Miner P, Coughlan R, Masum M, Shahriar H, Clincy V, Cetinkaya C (2021) Smart Connected aircraft: towards security, privacy, and ethical hacking. In 2021 14th International Conference on Security of Information and Networks (SIN). IEEE, pp 1:1–5. https://doi.org/10.1109/SIN54109.2021.9699243

Finkle J (2014) Hacker says to show passenger jets at risk of cyberattack. Available at: https://www.reuters.com/article/idUSKBN0G40WQ/. Accessed 6 Jan 2024

Florido-Benítez L (2016) Mobile apps: improve airports´ brand image and differentiate among competitors. ARA Tour Re 6:39–53. https://dialnet.unirioja.es/servlet/articulo?codigo=6852870. Accessed 1 May 2024

Florido-Benítez L (2020) Aeropuerto de Sevilla: un éxito de buena gestión de relación e interoperabilidad en la mejora de la conectividad aérea. Re.de Tur. Es. e Prá. 5, 1–30. http://geplat.com/rtep/index.php/tourism/article/view/631

Florido-Benítez L (2021) Identifying cybersecurity risks in Spanish airports. Cyber Security 4:267–291

Florido-Benítez L (2022) The safety-hygiene air corridor between UK and Spain will coexist with COVID-19. Logistics 6:52. https://doi.org/10.3390/logistics6030052

Florido-Benítez L (2023a) A Bibliometric Overview of the International Airports and Airlines 'IAA' Topic in Journals and Scientific Community. Logistics 7:35. https://doi.org/10.3390/logistics7030035

Florido-Benítez L (2023b) The role of the Top 50 US cargo airports and 25 air cargo airlines in the logistics of e-commerce companies. Logistics 7:8. https://doi.org/10.3390/logistics7010008

Florido-Benítez L (2023c) Cleaning and hygiene in the Air transport industry after the COVID-19 pandemic. Hygiene 3:383–395. https://doi.org/10.3390/hygiene3040028

Florido-Benítez L (2023d) English, German, and French Tourists are key to the success of Andalusian destinations (Spain). Sustainability 15:12521. https://doi.org/10.3390/su151612521

Florido-Benítez L (2024) The cybersecurity applied by online travel agencies and hotels to protect users' private data in smart cities. Smart Cities 7(1):475–495. https://doi.org/10.3390/smartcities7010019

Florido-Benítez L, Aldeanueva Fernández I (2022) Fusing international business and marketing: a bibliometric study. Adm Sci 12:159. https://doi.org/10.3390/admsci12040159

Florido-Benítez L, del Alcázar B (2015) The effects of apps as a marketing tool in airport infrastructure and airlines. Inter J Le Tour Mar 4:222–240. https://doi.org/10.1504/IJLTM.2015.072118

Gandhi F, Pansaniya D, Naik, (2022) Ethical hacking: types of hackers, cyberattacks and security. Int Res In En Tec 6:28. https://doi.org/10.47001/IRJIET/2022.601007

Gatlan S (2019) European airport systems infected with monero-mining malware. Available at: https://www.bleepingcomputer.com/news/security/european-airport-systems-infected-with-monero-mining-malware/. Accessed 19 Jan 2024).

Glen L (2023) The motivations of a hacker. Available at: https://focusgroup.co.uk/resources/blog/motivations-of-a-hacker/#:~:text=Cash,personal%20data%2C%20and%20trade%20secrets. Accessed 17 Jan 2024

Graphus (2022) 10 facts about insider risk that you must see. Available at: https://www.graphus.ai/blog/10-facts-about-insider-risk-that-you-must-see/. Accessed 16 Jan 2024

Greig J (2022) Experts push back on TSA's 24-hour cybersecurity incident reporting rule for aviation industry. Available at: https://therecord.media/experts-push-back-on-tsas-24-hour-cybersecurity-incident-reporting-rule-for-aviation-industry. Accessed 23 Jan 2024

Groos G (2003) FAA: Slammer didn't hurt us, but other attacks coming. Available at: https://www.networkworld.com/article/894123/lan-wan-faa-slammer-didn-t-hurt-us-but-other-attacks-coming.html. Accessed 8 Jan 2024

Hagos E, Brijs T, Brijs K, Wets G, Teklu B (2023) Safety Culture among Transport Companies in Ethiopia: Are They Ready for Emerging Fleet Technologies? Sustainability 15:3232. https://doi.org/10.3390/su15043232

Hancock J (2020) Understand the mistakes that compromise your company's security. Available at: https://www.tessian.com/research/the-psychology-of-human-error/. Accessed 5 Jan 2024

Hardcastle JL (2023) 'Russian hacktivists' brag of flooding German airport sites. Available at: https://www.theregister.com/2023/02/17/german_airport_websites_ddos/. Accessed 2 Jan 2024

Hétu DD, Morselli C, Leman-Langlois S (2012) Welcome to the scene: a study of social organization and recognition among warez hackers. J Re Cri De 49:359–382. https://doi.org/10.1177/0022427811420876

HITBSECCONF2013 Amsterdam (2021) Hacking the planet with knowledge graphs - Hugo Teso. Available at: https://youtu.be/Q6BkFNaXEVQ?feature=shared. Accessed 12 Jan 2024

Holt TJ (2007) Subcultural evolution? examining the influence of on- and off-line experiences on deviant subcultures. De Be 28:171–198. https://doi.org/10.1080/01639620601131065

Holt TJ (2009) The attack dynamics of political and religiously motivated hackers. Cy In Pro 161182:159–180. http://www.jstor.com/stable/resrep11979.10. Accessed 6 July 2024

Holt TJ, Bossler AM (2008) Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. De Be 30:1–25. https://doi.org/10.1080/01639620701876577

Holt TJ, Kilger M (2008) Techcrafters and makecrafters: A comparison of two populations of hackers. In 2008 WOMBAT workshop on information security threats data collection and sharing. IEEEE, pp 67–78. https://doi.org/10.1109/WISTDCS.2008.9

Holt TJ, Leukfeldt R, van de Weijer S (2020) An examination of motivation and routine activity theory to account for cyberattacks against Dutch web sites. Cri l Ju Be 47:487–505. https://doi.org/10.1177/0093854819900322

Holt TJ, Griffith M, Turner N, Greene-Colozzi E, Chermak S, Freilich JD (2023) Assessing nation-state-sponsored cyberattacks using aspects of Situational Crime Prevention. Cri Pu Po 22:825–848. https://doi.org/10.1111/1745-9133.12646

Homeland Security Today (2023) Long beach airport's website taken down by cyberattack. Available at: https://www.hstoday.us/subject-matter-areas/transportation/long-beach-airports-website-taken-down-by-cyber-attack/. Accessed 23 Jan 2024

Hunker J, Probst CW (2011) Insiders and insider threats-an overview of definitions and mitigation techniques. J Wirel Mob Ne Ubi Co De Appl 2:4–27

HYCU (2023) Ransomware attacks - never pay the ransom (Here's Why). Available at: https://www.hycu.com/blog/ransomware-attacks-dont-pay-the-ransom#:~:text=Organizations%20must%20also%20be%20aware,of%20Foreign%20Assets%20Control%27s%20regulations. Accessed 22 Jan 2024

IATA (2023) Annual review 2023. Available at: https://www.iata.org/contentassets/c81222d96c9a4e0bb4ff6ced0126f0bb/annual-review-2023.pdf. Accessed 5 Jan 2024

ICAO (2022) Aviation cybersecurity. Available at: https://www.icao.int/aviationcybersecurity/Pages/default.aspx. Accessed 24 Jan 2024

IMARC Group (2024) Aviation cybersecurity market report by solution type. Available at: https://www.imarcgroup.com/aviation-cyber-security-market. Accessed 6 Jan 2024

Infosecurity Magazine (2008) FAA plays down boeing 787 security concerns. Available at: https://www.infosecurity-magazine.com/news/faa-plays-down-boeing-787-security-concerns/. Accessed 20 Jan 2024

Jamieson KH (2020) Cyberwar: how Russian hackers and trolls helped elect a president: what we don't, can't, and do know. Oxford University Press

Jayakumar S (2020) Cyberattacks by terrorists and other malevolent Actors: prevention and preparedness with three case studies on Estonia, Singapore, and the United States. Handbook of Terrorism Prevention and Preparedness, pp 871–925

Kagalwalla N, Churi PP (2019) Cybersecurity in aviation: an intrinsic review. In 2019 5th International Conference on computing, communication, control and automation (ICCUBEA) IEEE, 1–6. https://doi.org/10.1109/ICCUBEA47591.2019.9128483

Karamitsos I, Papadaki M, Al-Hussaeni K, Kanavos A (2023) Transforming airport security: enhancing efficiency through blockchain smart contracts. Electronics 12:4492. https://doi.org/10.3390/electronics12214492

Karpersky (2023) What is hacking? And how to prevent it. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-hacking. Accessed 19 Jan 2024

Kaspersky (2023a) Stuxnet explained: what it is, who created it and how it works. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet. Accessed 11 Jan 2024

Kaspersky (2023b) Top 10 most notorious hackers of all time. Available at: https://www.kaspersky.com/resource-center/threats/top-ten-greatest-hackers. Accessed 9 Jan 2024

Kaspersky (2023c) Black hat, White hat, and gray hat hackers – definition and explanation. Available at: https://www.kaspersky.com/resource-center/definitions/hacker-hat-types. Accessed 9 Jan 2024
Kissel R (2011) 2011. Diane Publishing, Glossary of key information security terms
Klenka M (2021) Aviation cybersecurity: legal aspects of cyberthreats. J Transp Secur 14:177–195. https://doi.org/10.1007/s12198-021-00232-8
KonBriefing (2022) Cyberattacks on the aviation industry in 2022. Available at: https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html. Accessed 1 Jan 2024
Le Coze JC (2022) The 'new view' of human error. Origins, ambiguities, successes, and critiques". Sa Scie 54:105853. https://doi.org/10.1016/j.ssci.2022.105853
Lehto M (2020) Cybersecurity in aviation, maritime and automotive. In: Diez P, Neittaanmäki P, Periaux J, Tuovinen T, Pons-Prats J (eds) Computation and big data for transport. Computational methods in applied sciences, vol 54. Springer, Cham p 19–32. https://doi.org/10.1007/978-3-030-37752-6_2
Leśnikowski W (2021) Threats from cyberspace for civil aviation. Wi Obro 276:124–153
Lewis TG (2019) Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons
Lezzi M, Lazoi M, Corallo A (2018) Cybersecurity for Industry 4.0 in the current literature: a reference framework. Co In 103:97–110. https://doi.org/10.1016/j.compind.2018.09.004
Lindsay JR (2017) Cyberespionage. The Oxford Handbook of Cybersecurity. Oxford University Press, UK Oxford
Loh W (2023) Anonymity, fidelity to law, and digital Civil disobedience. Phi so Cri 49:448–476. https://doi.org/10.1177/01914537211072886
Loper K (2022) The criminology of computer hackers: a qualitative and quantitative analysis.Unpublished dissertation, Michigan State University, East Lansing, Michigan
Lykou G, Anagnostopoulou A, Gritzalis D (2018a) Smart airport cybersecurity: threat mitigation and cyber resilience controls. Se Ba 19:19. https://doi.org/10.3390/s19010019
Lykou G, Anagnostopoulou A, Gritzalis D (2018b) Implementing cybersecurity measures in airports to improve cyber-resilience. In 2018 Global Internet of Things Summit (GIoTS). IEEE, pp 1–6. https://doi.org/10.1109/GIOTS.2018.8534523
Lykou G, Moustakas D, Gritzalis D (2020) Defending airports from UAS: a survey on cyber-attacks and counter-drone sensing technologies. Sensors 20:3537. https://doi.org/10.3390/s20123537
Maalsen S (2022) The hack: What it is and why it matters to urban studies. Ur Stu 59:453–465. https://doi.org/10.1177/0042098020986300
Mannes M (2023) Airline SAS network hit by hackers, says app was compromised. Available at: https://www.reuters.com/business/aerospace-defense/airline-sas-suffers-cyber-attack-customer-info-leaked-2023-02-14/. Accessed 16 Jan 2024
McAlaney J, Hambidge S, Kimpton E, Thackray H (2020) Knowledge is power: an analysis of discussions on hacking forums. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, pp 477–483
Memis I (2024) Cybersecurity for airports: safeguarding against today's threats. Available at: https://www.beumergroup.com/knowledge/airport/cybersecurity-for-airports-safeguarding-against-todays-threats/. Accessed 17 Jan 2024
Meyer S (2018) Airline data breaches worrying. Available at: https://www.cpomagazine.com/cyber-security/airline-data-breaches-worrying/. Accessed 22 Jan 2024
Microsoft (2023) Microsoft digital defense report 2023. Available at: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023. Accessed 18 Jan 2024
Milan S (2013) Social movements and their technologies: Wiring social change. Palgrave Macmillan, London
Mooren L, Grzebieta RH (2010) Safety review of a dangerous goods transport company: a case study. In Proceedings of the Australasian road safety research, policing, and education conference. Monash University, p.14.
Mukhopadhyay A, Jain S (2024) A framework for cyber-risk insurance against ransomware: A mixed-method approach. Inter J In Ma 74:102724. https://doi.org/10.1016/j.ijinfomgt.2023.102724
Niraula, M. (2022). Cybersecurity and Interoperability of Aviation Safety Service Ecosystem. In *2022 Integrated Communication, Navigation and Surveillance Conference (ICNS)*. IEEE. pp. 1–12. https://doi.org/10.1109/ICNS54818.2022.9771482
Nobles, C (2019) Cyberthreats in civil aviation. In Emergency and Disaster Management: Concepts, Methodologies, Tools, and Applications (pp 119–141). IGI Global

Omolara AE, Alawida M, Abiodun OI (2023) Drone cybersecurity issues, solutions, trend insights and future perspectives: a survey. Ne Co App 35:23063–23101. https://doi.org/10.1007/s00521-023-08857-7

Pačka R, Miroslav Mareš M (2023) Achieving cyber power through integrated government capability: factors jeopardizing civil-military cooperation on cyberdefense. J Ap Se Re 18:436–461. https://doi.org/10.1080/19361610.2021.2006033

Paganini P (2013) Istanbul Ataturk international airport targeted by a cyberattack. Available at: https://securityaffairs.com/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html. Accessed 7 Jan 2024

Paganini P (2019) Ecuador suffered 40 million cyberattacks after the Julian Assange arrest. Available at: https://securityaffairs.com/83940/hacktivism/julian-assange-arrest-ddoss.html. Accessed 17 Jan 2024

Paganini, P (2024) A cyberattack hits the Beirut International airport. Available at: https://securityaffairs.com/157079/hacking/cyber-attack-hit-beirut-international-airport.html. Accessed 3 Jan 2024

Papathanasiou A, Liontos G, Liagkou V, Glavas E (2023) Business email compromise (BEC) attacks: threats, vulnerabilities and countermeasures—a perspective on the greek landscape. J Cybersecur Priv 3:610–637. https://doi.org/10.3390/jcp3030029

Pashel BA (2007) Teaching students to hack: Ethical implications in teaching students to hack at the university level. In Proceedings of the 2006 Information Security Curriculum Development Conference, InfoSecCD '06, Kennesaw, Georgia, 22–23 September 2006; Association for Computing Machinery: New York, NY, USA. pp 197–200. https://doi.org/10.1145/1231047.1231088?casa_token=jvdicHfLcz8AAAAA:BB9LIbdUERnxgD21OjGNuce0-InWmi1qDO7IT_F3RbM6PS19Aqbo2edW03SauMtZF_jLiR__v9qe_Q

Patterson CM, Nurse JR, Franqueira VN (2024) "I don't think we're there yet": The practices and challenges of organizational learning from cyber security incidents. Co Se 139:103699. https://doi.org/10.1016/j.cose.2023.103699

Phillips P, Champion J, Bettle P (2022) Aviation is facing a rising wave of cyber-attacks in the wake of COVID. Available at: https://www.shlegal-aviation.com/insight/aviation-facing-rising-wave-cyber-attacks-wake-covid. Accessed 23 Jan 2024

Prasad ST (2014) Ethical hacking and types of hackers. *Inter.E. Te.Co*. Sci Ele 11:24–27

Rawal BS, Manogaran G, Peter A (2023) Hacking for dummies. In: Cybersecurity and Identity Access Management. Springer, Singapore, pp 47–62. https://doi.org/10.1007/978-981-19-2658-7_3

Reed J (2023) Increasing insider cyberthreats pose risks to aviation. https://www.aviationtoday.com/2023/06/14/increasing-insider-cyber-threats-pose-risks-to-aviation/. Accessed 20 Jan 2024

Reuters (2017) British airways I.T. outage caused by contractor who switched off power – Times. Available at: https://www.reuters.com/article/idUSKBN18T0L6/. Accessed 17 Jan 2024

Reuters (2022) Hacker attack hits airport services provider Swissport. In: https://www.reuters.com/article/idUSKBN2K914T/. Accessed 13 Jan 2024

Rogers M, Smoak N, Liu J (2006) Self-reported computer deviant behaviour: a bit-5, moral choice, and manipulative exploitive behaviour analysis. De Be 27:245–268. https://doi.org/10.1080/01639620600605333

Romagna M (2020) Hacktivism: conceptualization, techniques, and historical view. The Palgrave handbook of international cybercrime and cyberdeviance. Bossler Ada, pp 743–769

Ronickher A, LaGarde M (2023) Whistleblower. Available at: https://katzbanks.com/wp-content/uploads/cybersecurity-whistleblower-protection-guide.pdf. Accessed 16 Jan 2024

Sabeel U, Heydari SS, El-Khatib K, Elgazzar K (2023) Unknown, atypical and polymorphic network intrusion detection: a systematic survey. IEEE Trans Netw Serv Manag. https://doi.org/10.1109/TNSM.2023.3298533

Sangwan RS, Badr Y, Srinivasan SM (2023) Cybersecurity for AI systems: a survey. J Cybersecur Priv 3:166–190. https://doi.org/10.3390/jcp3020010

Satariano A (2019) After a data breach, British airways faces a record fine. Available at: https://www.nytimes.com/2019/07/08/business/british-airways-data-breach-fine.html. Accessed 17 Jan 2024

Schia NN, Gjesvik L (2020) Hacking democracy: managing influence campaigns and disinformation in the digital age. J Cy Po 5:413–428. https://doi.org/10.1080/23738871.2020.1820060

Schmidt AV (2016) Cyberterrorism: combating the aviation industry's vulnerability to cyberattack. Su Tra Law Rev 39:169

Schoenherr JR (2022) Insider threats and individual differences: Intention and unintentional motivations. IEEE Tra Te So 3:175–184. https://doi.org/10.1109/TTS.2022.3192767
SecurityBrief (2021) A brief history of cyber-threats — from 2000 to 2020. Available at: https://securitybrief.co.nz/story/a-brief-history-of-cyber-threats-from-2000-to-2020#:~:text=First%2C%20there%20was%20the%20ILOVEYOU,to%20%2415%20billion%20in%20damages. Accessed 2 Jan 2024
Sharma P, Barua S (2023) From data breach to data shield: the crucial role of big data analytics in modern cybersecurity strategies. Inter J In Cyber 7:31–59. https://publications.dlpress.org/index.php/ijic/article/view/46. Accessed 22 June 2024
Sharma T, Patni K, Li Z, Trajković L (2023) Deep echo state networks for detecting internet worm and ransomware attacks. In 2023 IEEE International Symposium on Circuits and Systems (ISCAS). IEEE, pp 1–5. https://doi.org/10.1109/ISCAS46773.2023.10182056
Shimbun Y (2024) Suspicion of human error grows in Haneda airport collision; records indicate coast guard plane not told to enter runway. Available at: https://japannews.yomiuri.co.jp/society/general-news/20240104-159817/. Accessed 23 Jan 2024
Singh KD, Loura J (2022) Impact of covid-19 on operations and cyber-vulnerability of civil aviation. A J c Sci 5:34–39
Smith I (2023) Lloyd's finds major hack of a payments system could cost $3.5tn. Available at: https://www.ft.com/content/f4f09c0d-19aa-41c4-ac72-5f3395118960. Accessed 22 Jan 2024
Solomon S (2019) Israeli airports fend off 3 million attempted attacks a day, cyber head says. Available at: https://www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/. Accessed 11 Jan 2024
Soner O, Kayisoglu G, Bolat P, Tam K (2024) Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. App Oce Res 142:103855. https://doi.org/10.1016/j.apor.2023.103855
Suciu G, Scheianu A, Vulpe A, Petre I, Suciu V (2018) CyberAttacks – the impact over airports security and prevention modalities. In: Rocha Á, Adeli H, Reis L, Costanzo S (eds) Trends and Advances in Information Systems and Technologies. WorldCIST'18 2018. Advances in Intelligent Systems and Computing, vol 747. Springer, Cham, p 154–162. https://doi.org/10.1007/978-3-319-77700-9_16
Sukesh S, Mirian DH, Robin CR (2023) An analysis of the increasing cases of data breaches in India. J So Eng 17:19791
Surette J (2023) Cyberattacks are on the up: what are the risks & remedies for aviation? Available at: https://simpleflying.com/cyberattacks-risks-remedies-aviation/. Accessed 3 Jan 2024
Swinhoe D (2019) Why businesses don't report cybercrimes to law enforcement. Available at: https://www.csoonline.com/article/567307/why-businesses-don-t-report-cybercrimes-to-law-enforcement.html#:~:text=Businesses%20are%20underreporting%20cybercrimes&text=A%202016%20report%20by%20Barclays,were%20reported%20to%20the%20police. Accessed 21 Jan 2024
Teichmann FMJ, Sergi BS, Wittmann C (2023) The compliance implications of a cyberattack: a distributed denial of service (DDoS) attack explored. Int Cy Law Rev 4:291–298. https://doi.org/10.1365/s43439-023-00090-1
The hacker News (2018) Ransomware attack takes down Bristol airport's flight display screens. Available at: https://thehackernews.com/2018/09/cyberattack-bristol-airport.html. Accessed 21 Jan 2024
Timothy LT (2003) Al Qaeda and the Internet: the danger of cyberplanning. Parameters 23:112–123
Topham G (2019) Gatwick drone disruption cost airport just £1.4m. Available at: https://www.theguardian.com/uk-news/2019/jun/18/gatwick-drone-disruption-cost-airport-just-14m. Accessed 3 Jan 2024
Ukwandu E, Ben-Farah MA, Hindy H, Bures M, Atkinson R, Tachtatzis C, Andonovic I, Bellekens X (2022) CyberSecurity challenges in aviation industry: a review of current and future trends. Infor 13:146. https://doi.org/10.3390/info13030146
University of Denver (2023) The complete guide to ethical hacking. Available at: https://bootcamp.du.edu/blog/the-complete-guide-to-ethical-hacking/. Accessed 15 Jan 2024
US Department of Justice (2009) Former boeing engineer convicted of economic espionage in theft of space shuttle secrets for China. Available at: https://www.justice.gov/opa/pr/former-boeing-engineer-convicted-economic-espionage-theft-space-shuttle-secrets-china. Accessed 9 Jan 2024
US Department of Justice (2011) Impact of 9/11 terrorist attacks on research agenda. Available at: https://nij.ojp.gov/topics/articles/impact-911-terrorist-attacks-research-agenda. Accessed 11 Jan 2024
Varlioglu S, Elsayed N, ElSayed Z, Ozer M (2022) The dangerous combo: Fileless malware and crypto jacking. SoutheastCon 5:125–132. https://doi.org/10.1109/SoutheastCon48659.2022.9764043

Varshney G, Kumawat R, Varadharajan V, Tupakula U, Gupta C (2024) Anti-phishing: a comprehensive perspective. Expert Sys App 238:122199. https://doi.org/10.1016/j.eswa.2023.122199

Vishnuram G, Tripathi K, Tyagi AK (2022) Ethical hacking: importance, controversies and scope in the future. In 2022 International Conference on Computer Communication and Informatics (ICCCI). IEEE. 01–06. https://doi.org/10.1109/ICCCI54379.2022.9740860

Weathersby A (2023) Discerning the relative threat of different network based cyber-attacks, a study of motivation, attribution, and anonymity of hackers. ProQuest Dissertations & Theses Global. Available at: https://www.proquest.com/dissertations-theses/discerning-relative-threat-different-network/docview/2755904641/se-2. Accessed 17 Jan 2024

Weimann G (2004) Cyberterrorism. How real is the threat? Available at: https://www.usip.org/sites/default/files/sr119.pdf. Accessed 16 Jan 2024

Willard J (2023) Economic impact of cybercrime on business predicted to reach $10.5 trillion by 2025: Cybersecurity Ventures. Available at: https://www.reinsurancene.ws/economic-impact-of-cybercrime-on-business-predicted-to-reach-10-5-trillion-by-2025-cybersecurity-ventures/#:~:text=The%20economic%20impact%20of%20cybercrime,risk%20appears%20to%20be%20diminishing. Accessed 5 Jan 2024

Wilson Kehoe Winingham Team (2022) Aviation accidents: Human error. Available at: https://www.wkw.com/aviation-accidents/blog/aviation-accidents-human-error/. Accessed 21 Jan 2024

Withers K, Parrish J, Ellis T, Smith J (2020) Vice or virtue? Exploring the dichotomy of an offensive security engineer and government "hack back" policies. In: Proceedings of the 53rd Hawaii International Conference on System Sciences. pp 1813–1822. http://hdl.handle.net/10125/63963. Accessed 7 July 2024

Yannakogeorgos PA (2013) Strategies for resolving the cyber attribution challenge. Air University Press. https://www.hsdl.org/?view&did=811823. Accessed 17 July 2024

Żmigrodzka M (2020) Cybersecurity – one of the greatest challenges for civil aviation in the 21st century. Sa De 6:33–41. https://doi.org/10.37105/sd.73