information

Review

Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends

Elochukwu Ukwandu [1], Mohamed Amine Ben-Farah [2], Hanan Hindy [3], Miroslav Bures [4], Robert Atkinson [5], Christos Tachtatzis [5], Ivan Andonovic [5] and Xavier Bellekens [6,*]

1 Department of Applied Computing and Engineering, Cardiff School of Technologies, Cardiff Metropolitan University, Cardiff CF5 2YB, UK; eaukwandu@cardiffmet.ac.uk
2 Department of Networks and Cyber Security, Birmingham City University, Birmingham B5 5JU, UK; mohamed.benfarah@bcu.ac.uk
3 Computer Science Department, Faculty of Computer and Information Sciences, Ain Shams University, Cairo 11566, Egypt; hananhindy@ieee.org
4 Department of Computer Science, FEE, Czech Technical University in Prague, 166 36 Prague 6, Czechia; buresm3@fel.cvut.cz
5 Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow G1 1XW, UK; robert.atkinson@strath.ac.uk (R.A.); christos.tachtatzis@strath.ac.uk (C.T.); i.andonovic@strath.ac.uk (I.A.)
6 Lupovis Limited, Glasgow G2 2BA, UK
* Correspondence: xavier@lupovis.io

Abstract: The integration of Information and Communication Technology (ICT) tools into mechanical devices in routine use within the aviation industry has heightened cyber-security concerns. The extent of the inherent vulnerabilities in the software tools that drive these systems escalates as the level of integration increases. Moreover, these concerns are becoming even more acute as the migration within the industry in the deployment of electronic-enabled aircraft and smart airports gathers pace. A review of cyber-security attacks and attack surfaces within the aviation sector over the last 20 years provides a mapping of the trends and insights that are of value in informing on future frameworks to protect the evolution of a key industry. The goal is to identify common threat actors, their motivations, attacks types and map the vulnerabilities within aviation infrastructures most commonly subject to persistent attack campaigns. The analyses will enable an improved understanding of both the current and potential future cyber-security protection provisions for the sector. Evidence is provided that the main threats to the industry arise from Advance Persistent Threat (APT) groups that operate, in collaboration with a particular state actor, to steal intellectual property and intelligence in order to advance their domestic aerospace capabilities as well as monitor, infiltrate and subvert other sovereign nations' capabilities. A segment of the aviation industry commonly attacked is the Information Technology (IT) infrastructure, the most prominent type of attack being malicious hacking with intent to gain unauthorised access. The analysis of the range of attack surfaces and the existing threat dynamics has been used as a foundation to predict future cyber-attack trends. The insights arising from the review will support the future definition and implementation of proactive measures that protect critical infrastructures against cyber-incidents that damage the confidence of customers in a key service-oriented industry.

Keywords: aviation industry; cyber-security; threat dynamics; information and communication technology; cyber-incidents

Citation: Ukwandu, E.; Ben-Farah, M.A.; Hindy, H.; Bures, M.; Atkinson, R.; Tachtatzis, C.; Andonovic, I.; Bellekens, X. Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information* **2022**, *13*, 146. https://doi.org/10.3390/info13030146

Academic Editor: Sokratis Katsikas

Received: 10 February 2022
Accepted: 5 March 2022
Published: 10 March 2022

1. Introduction

The ongoing trend in increasing the levels of the integration of Information and Communication Technology (ICT) tools into mechanical devices in routine use within the aviation industry has surfaced concerns regarding the resilience of current cyber-security protection frameworks. Thus, consideration of the needs of the sector in terms of cyber-

security compliance is featuring as another challenge in the evolution of the aviation industry through the adoption of smart airports and e-enabled aircraft infrastructures [1].

The aviation industry holds a strategic global position as the gateway between nations. The resilience of the infrastructures in support of its operational integrity is vital as minor errors or oversights result in a range of significant damages and losses, e.g., fatalities, loss or exposure of stakeholders, staff and customer personally identifiable information, theft of credentials, intellectual property and intelligence. There is clear evidence, as shown in Sections 2.3 and 3, that major threat actors are collaborating with state actors to acquire intellectual property and intelligence, in order to advance their domestic aerospace capabilities as well as to monitor, infiltrate and subvert other nations' capabilities. Thus, there is an industry imperative to define and implement commensurate cyber-defense strategies that protect against malicious threats that endanger the operational integrity of a key industry.

Monteagudo [2] recommend the industry adopt micro-segmentation strategies in cyber-defence design and implementations, resulting in the division of aviation infrastructures into multiple micro-islands, each governed by separate access privileges. The approach targets the containment of any compromise or data breach to a specific segment. Bellekens et al. [3] propose a deception solution for the early detection of breaches in critical infrastructures as current techniques are ineffective, with threats to the civil aviation industry continuing to proliferate with a focus on stealing information for both political and financial gains, with some malicious acts resulting in long-term business disruptions [4].

The review explores the cyber-security landscape within the civil aviation industry only; military flight operations are not considered. Private and commercial areas of the industry are reviewed with consideration of the entire ecosystem, extending to the whole system of avionics, air-traffic controls, airlines, and airports. The goal is to provide a critical assessment of the current trends and practices and based on the results of the analyses, predict future trends as the civil aviation industry continues to increase the use of Information Technology (IT) technologies, such as Internet of Things (IoT) devices, machine learning, cloud storage and cloud computing, to optimise business operations.

The remainder of the review is organised as follows. Section 2 captures the range of reported cyber-threats, the threat actors and their motivation drawn from the published literature. Section 3 focuses on the documented cyber-attacks in the last 20 years, while Section 4 provides a mapping of the attack surfaces a malicious attacker can exploit—at the airport or in aircraft systems. Section 5 contains insight on the steps to mitigate cyber-security challenges within the civil aviation industry. Section 6 describes the future evolution of the civil aviation sector as it relates to smart airports and e-enabled aircraft, laying the environment for the prediction of the concomitant changes in the threat dynamics and their implications on the industry. Conclusions are drawn in Section 7, with Section 8 providing open research challenges and opportunities in civil aviation cyber-securities.

2. A Systematic Literature Review

Section 2 presents a review of the available literature on cyber-attack incidents, the threat actors and their motivation within the civil aviation industry.

2.1. Review Methodology

The review was executed following the process of systematic analysis and methodology defined by Okoli and Schabram in [5] and Okoli in [6], guiding the selection and extraction of relevant information from the literature. The objectives of the analysis is to map reported cyber-security incidents within private and commercial areas of the industry over the last 20 years (2001–2021), with consideration of the whole system of avionics, air-traffic controls, airlines, and airports.

2.1.1. Aim and Objectives

The aim is to identify and analyse reported cyber-security incidents across the aviation sector over the last 20 years (2001–2021) to benchmark the most common threat actors, their motivations, the class of attacks and the aviation infrastructure subject to most attacks. Insights on the current scenario lay the foundation with which to predict future cyber-security practices. The specific objectives are as follows:

- Survey of cyber-attack incidents in the civil aviation sector over the last 20 years;
- Analysis and review of state-of-the-art cyber-attack trends, threat actors and their motivation;
- Identification of the most common types of attacks and targeted infrastructures;
- Providing cyber-security professionals with information on the current and future trends of cyber-attack incidents in the context of the evolution of the civil aviation sector.

2.1.2. Classification and Research Criteria

A survey of peer-reviewed papers showed that a limited number of papers have been reported with regard to cyber-attack incidents in the civil aviation sector. As an example, only 1 publication was found in the Scopus database when searched using a combination of the following keywords 'cyber AND incident AND aviation AND industry'; and a total of 29 publications were found when searched using 'cyber AND attack AND aviation AND industry', of which 27 were journal articles and 2 were conference proceedings articles published in 2021. The trend in the number of relevant published papers shows a steady increase over the recent past; five journal and two conference proceedings articles were published in 2020; three journal and three conference proceedings articles in 2019; one journal/two conference proceedings articles in 2018; only three conference proceedings articles in 2017; one journal and one conference proceedings article were published in each of 2016, 2015 and 2013; and, finally, there was one publication as part of conference proceeding in 2012 and none thereafter. (Table 1). Worth noting is that no article focused on articulating cyber-attack incidents, rather propose different cyber-security approaches in securing the aviation infrastructure of both internal and external systems in the sector. Here, an extensive search was employed to surface relevant information from online repositories, web-based announcements, online articles and reports on websites of both primary and third-party organisations operating in aviation sectors. The review was supplemented by web-based aviation cyber-security reports, newspapers and news magazine, status reports, regulations and related information from regulatory agencies. The relevant incidents were tabulated based on the class of attack and according to the cyber-security triad of Confidentiality, Integrity and Availability. The source, year, location and type of attack, a more detailed description of the attack with the people affected and the possible cost implications for each incident were recorded.

Furthermore, the review considered only cyber-attacks over the last 20 years, namely, from 2001 to 2021, as the only other documented incident within the industry between 1997–2014 was theft of an MSc thesis.

The selected search term—the concatenation of keywords 'cyber AND incident AND aviation AND industry'—will exclude relevant literature that did not use/cite any of the keywords. Moreover, as the search is English-based, it excludes any potential non-English-language papers. The authors also acknowledge the possibility of excluding literature in databases with which their respective institutions have no established subscription.

2.2. Cyber-Threats and Automation in Civil Aviation Industry

Given the importance of cyber-technologies to the operational integrity of the aviation industry, the sector has relied on the International Air Transport Association (IATA) [7] to provide guidance to improve and update cyber-security regulations, standards, and principles for the end-to-end ecosystem comprising the whole system of avionics, air-traffic controls, airlines, and airports [2,8]. The business goals range from improving on-the-

ground/air-borne/in-space operations, customer services such as, but not limited to, ticket bookings, in-flight entertainment systems, flight check-in and -out, security screening of passengers and use of aircraft cabin wireless Internet services [8,9]. It is also evident that the use of a new suite of technologies and tools has yielded significant positive impacts on aircraft control systems, enhancing the quality of aviation operations, increasing safety and performance [2,9–12]. The trend, however, has concomitant negative impacts in terms of cyber-security through increasing vulnerabilities, gates which may result in breaches with potential losses in terms of human life and business continuity [2,12,13].

Table 1. Literature Search Results.

Year	Database	Journal	Conference	Total
2021	Scopus	1	2	3
2020	Scopus	5	2	7
2019	Scopus	3	3	6
2018	Scopus	1	2	3
2017	Scopus	0	3	3
2016	Scopus	1	1	2
2015	Scopus	1	1	2
2013	Scopus	1	1	2
2012	Scopus	0	1	1
Summary		13	16	29

In 2018, Corretjer [14] undertook an analysis of current cyber-security practices within the United States aviation industry (civil and military) and recorded the strategies of both government and private entities to protect the industry against cyber-attacks. The conclusions, although commending the effort to date of the Federal Airport Authority (FAA) and the private sector to manage the proliferation of cyber-attacks, recommend the need to intensify the implementation of proactive measures throughout the design, acquisition, operation and maintenance of aviation navigation systems.

Kagalwalla and Churi [15] stressed the increased challenges in provisioning cyber-security in aviation as a consequence of the increase in the deployment of modern ICT technologies such as IoT, machine learning, cloud storage/computing with their concomitant inherent vulnerabilities. Moreover, Duchamp, Bayram and Korhani [1] highlight that the increase in the number of travellers, building of new modern airports, and complexities in new aircraft have also stimulated an increase in cyber-attacks in civil aviation. ICAO [4] believe that the increased reliance on the integrity and confidentiality of data for the optimisation of day-to-day business transactions have in turn increased the risk of cyber-incidents. Increased levels of automation, a central spine within the evolution of next generation systems, result in the proliferation of attack surfaces with threat actors targeting business disruptions and theft of information for both political and financial gains.

Lehto [16] cites the dynamic between advancements in cyber-attack tools and methods coupled with increased exposures and the motivation of the attackers has created the current trend in cyber-attacks impacting airlines, aircraft manufacturers and authorities. Cyber Risk International [17] contend that the rise in cyber-security challenges is the result of a combination of digital transformation, higher levels of inter-connectivity, segmentation, and complexity, recent solutions by the industry to service the surge in global travel. In summary, the main conclusions reached are as follows: the heavy reliance on IT facilities to maintain quality of services has resulted in higher levels of exposure to cyber-attacks; multiple entry and exit in the industry creates new vulnerabilities; legacy IT issues and fragmentation significantly exacerbate the challenges as they were not designed

to cope with cyber-crime [2]. Kagalwalla and Churi [15] cite that the lack of resources, funds and skilled staff are part of the spectrum of challenges, as are insider threats, the procurement of modern-day operational technologies such as Supervisory Control and Data Acquisition (SCADA), Industrial Control Systems (ICS). Building a strong security culture, implementing meaningful prevention, and proactive measures are solutions that are offered.

2.3. Threat Actors and Their Motivations

Fireeye Incorporated [18] reported their findings on the major threat actors in the aerospace industry and the motives behind their attacks. The main finding of the assessment was that the most prevalent industry cyber threats arise from Advance Persistent Threat (APT) groups that work in collaboration with state actors to acquire intellectual property and intelligence in order to advance their domestic aerospace capabilities as well as to monitor, infiltrate and subvert other sovereign nations' capabilities. APTs were executed by cyber-espionage groups that specialise in targeting information and security assets of critical economic importance to nations and large corporations [19]. These groups are highly skilled, very knowledgeable, and experienced in carrying out malicious acts with high degrees of expertise in masking their attack paths, a mix of characteristics that render them elusive, high-profile and able to inflict significant damage. Evidence was provided that some groups operating in partnership with particular state actors, use the stolen assets to develop cyber-security countermeasures as well as technologies and tools for sale on the dark web. According to Fireeye's threat intelligence system, at least 24 APT incidents were identified that compromised different aerospace organisations with stolen data types ranging from budget information, business communications, equipment maintenance records and specifications. Other data include organisational charts and company directories, personally identifiable information, product designs, product blueprints, production processes and proprietary product or service information, research reports, safety procedures, system log files and testing results and reports, potentially enabling a spectrum of damaging consequences.

Kessler and Craiger [20] categorised the threat actors according to their motivations: cyber-criminals, whose activities are responsible for 450 billion dollars of annual loss to the global economy; cyber-activists/hacktivists whose concern is the philosophy, politics and non-monetary goals of the discipline; cyber-spies, motivated by financial, industrial, political and diplomatic espionage; and cyber-terrorists, driven by political, religious, ideological or social violence. Attackers supported by a nation-state in order to advance the latter's strategic goals are classified as cyber-warriors. Abeyratne [21] notes that threat actors are motivated by the ability to cause business disruption and theft of information for political as well as financial gains.

Recent reports reinforce the likelihood of a significant rise in cyber-threats as the volume of global passengers rises, with embedded systems being deployed in response in order to sustain the quality of services. The integration of hardware and software to increase the efficiency of operations through increased levels of automation presents a more extensive attack surface, stimulating further, the motivation of threat actors. It is therefore timely to accentuate the significant challenges facing the civil aviation industry in the provision of cyber-security as the number and classes of cyber-threats proliferate. The growing degree of threat should be addressed as a matter of urgency through research and innovation in proactive approaches within cyber-security by design tools that mitigate the risks and dissuade malicious activity.

3. Documented Cyber-Attacks in Aviation Industry (2001–2021)

The ever-increasing reliance in data-driven processes to increase the efficiency of businesses practices and the quality of life for citizens brings attendant risks and challenges in providing effective cyber-security protection [22]. It is clear that the integration of technologies has also increased the safety and efficiency of air transport systems. However,

higher levels of human migration and hyperconnectivity gate a cascading impact as a cyber-incident in one airport translates into a transnational problem with social and economic consequences [1]. It is therefore incumbent on the industry to be proactive in providing robust mitigation for any class of emergent attack.

In this context, Table 2 present reviews of documented cyber-threats and attacks in civil aviation industry over the last 20 years (2001–2021). The review by Viveros [23], which covered the period 1997–2014, is not exhaustive, as well as being outdated considering the evolutionary progression of cyber-security incidents in recent times. Although the presented mapping has been carried out diligently, the authors acknowledge the possibility that some cyber-attacks in the civil aviation industry within the period under review may have been omitted, as some incidents may not have been made public.

Table 2. Cyber-Attacks in the Civil Aviation Industry.

Class	Ref	Year	Incident	Source	Location	Description
C	[24]	2003	Slammer Worm attack	OTR	USA	One of the FAA's administrative servers was compromised through a slammer worm attack. Internet services were shut down in some parts of Asia as a result of this attack and this slowed down connections worldwide.
A	[25]	2006	Cyber-Attack	OTR	Alaska, USA	Two separate attacks on US Federal Aviation Administration (FAA) internet services that forced it to shut down some of its air traffic control systems.
C	[25]	2008	Malicious hacking attack	OTR	Oklahoma, USA	Hackers stole the administrative password of FAA's interconnected networks when they took control of their system. By gaining access to the domain controller in the Western Pacific region, they were able to access more than 40,000 login credentials used to control part of the FAA's mission-support network.
C	[26]	2009	Malicious hacking attack	OTR	USA	A malicious hacking attack on FAA's computer, through which hackers gained access to personal information of 48,000 current and former FAA employees.
C	[27]	2013	Malware attack	OTR	Istanbul, Turkey	Shutting down of passport control system at the departure terminals of Istanbul Ataturk and Sabiha Gokcen airports due to a malware attack, leading to the delay of many flights.
C	[28]	2013	Hacking and phishing attacks	OTR	USA	Malicious hacking and phishing attacks that targeted about 75 airports. These major cyber-attacks were alleged to have been carried out by an undisclosed nation-state that sought to breach US commercial aviation networks.
A	[29]	2015	DDoS attack	OTR	Poland	A Distributed Denial-of-Service (DDoS) attack by cyber-criminals that affected LOT Polish Airlines flight-plan IT Network systems at the Warsaw Chopin airport. The attack rendered LOT's system computers unable to send flight plans to the aircraft, thus grounding at least 10 flights, leaving about 1400 passengers stranded.
I	[30]	2016	Hacking, phishing attacks	OTR	Vietnam	The defacement of a website belonging to Vietnam airlines and flight information screens at Ho Chi Minh City and the capital, Hanoi, displaying messages supportive of China's maritime claims in the South China Sea by Pro-Beijing hackers.

Table 2. *Cont.*

Class	Ref	Year	Incident	Source	Location	Description
A	[31]	2016	Cyber-attack	OTR	Boryspil, Ukraine	A malware attack was detected in a computer in the IT network of Kyiv's main airport, which includes the airport's air traffic control system.
A	[30]	2017	Human error	OTR	United Kingdom	British flag-carrier computer systems failure caused by disconnection and re-connection of the data-center power supply by a contracted engineer. This accident left about 75,000 passengers of British Airways stranded.
C	[32]	2018	Data breach	OTR	Hong Kong	Cathay Pacific Airways data breach of about 9.4 million customers' personal identifiable information.
C	[33]	2018	Data breach	OTR	United Kingdom	British Airways Data breach of about 380,000 customers' personal identifiable information.
C	[34]	2018	Data breach	OTR	USA	Delta Air Lines Inc. and Sears Departmental stores reported a data breach of about 100,000 customers' payment information through a third party.
A	[35]	2018	Ransomware attack	OTR	Bristol Airport, UK	An attack on electronic flight information screens at Bristol Airport. This resulted in the screen being taken offline and replaced with whiteboard information. There was no known adverse effect from this attack.
C	[36]	2018	Mobile app data breach	OTR	Air Canada, Canada	Air Canada reported a mobile app data breach affecting the personal data of 20,000 people.
C	[37]	2018	Data breach	OTR	Washington DC, USA	Data breach on a NASA server that led to possible compromise of stored personally identifiable information (PII) of employees on 23 October 2018.
C	[38]	2018	Ransomware attack	OTR	Chicago, USA	Boeing was hit by the WannaCry computer virus, but the attack was reported to have minimal damage to the company's internal systems.
A	[20]	2018	Cyber-attack	TP	Sweden	Cyber-attack launched by Russian APT group (APT28) that blocked Sweden's air traffic control capabilities, grounding hundreds of flights over a 5-day period.
A	[39]	2019	Bot attacks	OTR	Ben Gurion Airport, Israel	About 3 million bots attacks were blocked in a day by Israel's airport authority, as they attempted to breach airport systems.
C	[40]	2019	Cyber-Incident	OTR	Toulouse, France	A cyber incident that resulted in unauthorised access to Airbus "Commercial Aircraft business" information systems. There was no known impact according to the report on Airbus' commercial operations.
C	[41]	2019	Ransomware attack	OTR	Albany, USA	Albany International Airport experienced a ransomware attack on Christmas of 2019. The attackers successfully encrypted the entire database of the airport forcing the authorities to pay a ransom in exchange of the decryption key to a threat actor.
C	[42]	2019	Crypto mining Malware infection	OTR	Europe	Cyberbit researchers discovered through their security software, known as EDR, a network infection of more than 50% of the European airport workstations by a cryptocurrency mining malware.

Table 2. *Cont.*

Class	Ref	Year	Incident	Source	Location	Description
C	[43]	2019	Phishing attack	OTR	New Zealand	A phishing attack targeted at Air New Zealand Airpoints customers. This attack compromised the personal information of approximately 112,000 customers, with names, details and Airpoints numbers among the data exposed.
C	[44]	2020	Ransomware attack	OTR	Denver, USA	A cyber-incident that involved the attacker accessing and stealing company data, which were later leaked online.
C	[45]	2020	Ransomware attack	OTR	San Antonio, USA	Data breach suffered by ST Engineering's aerospace subsidiary in the USA that later lead to a ransomware attack by Maze Cyber-criminal.
I	[46]	2021	Software Error	OTR	Birmingham, United Kingdom	A software error in the IT system that could not recognise mass discrepancies between loadsheet and the flight plan, leading to the aircraft having 1606 kg more take-off mass than required.

C = Confidentiality, I = Integrity, A = Availability, OTR = Online Technical Report and News, TP = Technical Presentation.

Analysis and Critical Reviews of Cyber-Attacks in the Civil Aviation Industry

Of all attacks studied, 71% focused on the theft of login details such as administrative passwords and malicious hacking to gain unauthorised access to the IT infrastructure (Figure 1). Denial-of-service attacks, such as Distributed Denial of Services (DDoS), which compromise data availability, rank second at 25%, followed by attacks that target corrupting the integrity of files, either by intercepting them while in transit or at rest, which correspond to 4% of all attacks. This evidence adds credence to the assertions presented in Section 2.3, which posits that the major motivation of threat actors is the theft of intellectual property and intelligence.

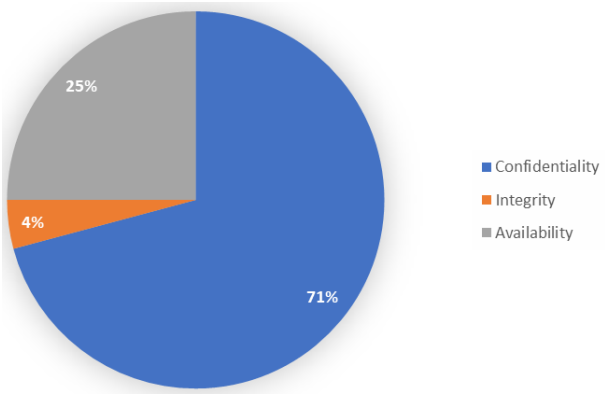

Figure 1. Cyber-Attack Class based on Security Triad.

The assessment of cyber-attack by type is presented in Figure 2, the results of which support the evidence presented in Figure 1, showing that malicious hacking activities top the list of the type of cyber-attacks at 26%, the aim being to gain unauthorised access using known malicious password cracking techniques, for example, brute force or dictionary attacks. Data breach and ransomware attacks are second at 14% each, while attacks related to phishing and malware follow at 11% each. Cyber-incidents classed as human error, bot attacks, worms and DDoS are the most rare, at 4% each.

Figure 3 shows that most cyber-attacks within the aviation industry occur in North America, with 11 out of 26 recorded incidents in the United States of America (USA) and

1 only in Canada. Mazareanu [47] suggests that the relatively large number of incidents may not be unconnected to the large number of airports in the USA, as in 2019, USA was home to 5080 public and 14,556 private airports. Europe is second with a 44% rate of attack incidents, with Britain topping the list of countries. Nations in Asia come third at 8%, with no known cyber-attacks recorded in airports in Africa. Table 3 captures the number of individuals impacted, the number of times airports were shut down, and the number of days aircraft were grounded owing to cyber-incidents. Incidents during 2018 remain the most numerous, representing the highest rate of cyber-attacks in the history of the aviation industry, with 94,500,000 people affected and about 5 continuous days of aircraft being grounded. The crypto-mining malware discovered by Cyberbit through its Endpoint Detection and Response (EDR) software in 2019 was, however, the most worrying incident, an installation of malicious software that infected more than 50% of the European airport workstations.

Table 3. Cost of Cyber-Attacks in the Aviation Industry Per Year.

Year	No. of Persons Affected	Airports Shut Down	Lost Flight Hours
2003	Not Provided	Not Provided	Not Provided
2006	Not Provided	2	Not Provided
2008	40,000	Not Provided	Not Provided
2009	48,000	Not Provided	Not Provided
2013	Not Provided	77	Not Provided
2015	1400	Not Provided	Not Provided
2016	Not Provided	Not Provided	Not Provided
2017	75,000	Not Provided	Not Provided
2018	94,500,000	Not Provided	120
2019	112,000	Not Provided	Not Provided
2020	Not Provided	Not Provided	Not Provided

Legend: Not Provided = records were not made public.

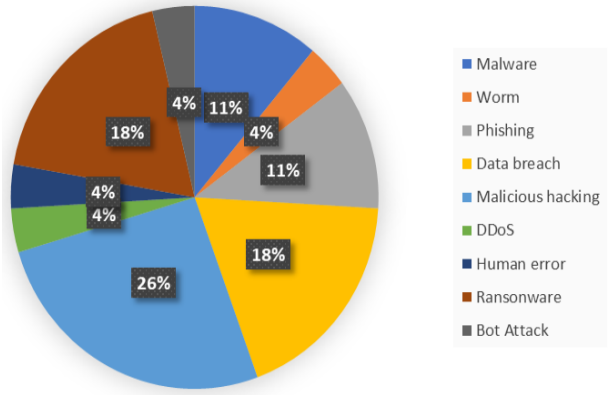

Figure 2. Cyber-Attacks by Type.

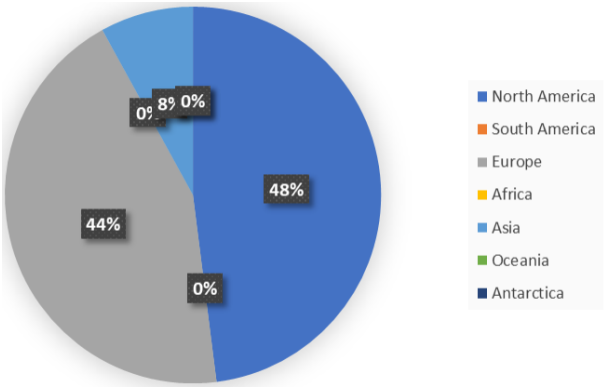

Figure 3. Cyber-Attacks by Location.

A quantification of losses owing to cyber-security breaches is hindered by the lack of transparency in record keeping, documentation and publication of relevant incidents for public knowledge. The monetary value of losses paid by the industry due to cyber-crime are never publicised, nor documented, especially the level of compensation to victims of these attacks, as well as that paid as ransom during ransomware attacks. Other records not disclosed are the number of shutdowns suffered by the attacked airports, as well as the number of lost flight hours as a consequence of cyber-incidents.

4. Cyber-Attack Surfaces and Vulnerabilities in the Civil Aviation Industry

Paganini [48] attests that only attackers with a broad understanding of how an aircraft or aviation system functions can successfully disrupt normal operations, citing that an attack on an entire aircraft or aviation system is non-trivial. Haass, Sampigethaya and Capezzuto [8] highlighted that technologies such as Wireless Fidelity (WiFi), Internet, IoT, Global Positioning System (GPS), open-source systems, virtualisation and cloud computing services have been central in the optimisation of aviation operations, reducing costs and response times through enhanced inter-operability. Integrated systems, however, can be targeted remotely due to their inherent vulnerabilities, an assertion shared by [2,49] and Lykou et al. [9]. Lykou et al. [9] also added that the practise of Bring Your Own Device (BYOD) by airport customers, travellers and employees creates a rich attack surface. As an example, the work in [50] reports an attacker's access of the in-flight entertainment by simply attaching a cat6 cable with a modified connector through his laptop; other aeroplane network systems could also be commandeered, as confirmed by Freiherr in [51].

Efe, Cavlan and Tuzlupinr [52] postulate that the increase in the number of operational aircraft coupled with the innovation driving the development of smaller and more sustainable air vehicles render air communication protocols a high-profile target for cyber-attacks. Duchamp, Bayram and Korhani [1], Kessler et al. [20] and Abeyratne [21] are of the view that the reliance on computer-based IT systems in the day-to-day management of the industry—which has enabled improvements in the sophistication of air navigation, on-board aircraft control and communication systems—increase the cyber-attack surface. Furthermore, airport ground systems, which include flight information, security screening and day-to-day data management systems, are also identified as targets. An aggregation of the above targets comprises the spectrum of feasible attack surfaces in the Civil Aviation Industry (CAI), with associated vulnerabilities.

Santamarta [53] discovered security flaws in Inmarsat and Iridium Satellite Communication (SATCOM) terminals in 2014, infrastructure in routine use within the aviation industry. Researchers concluded that malicious attackers have the potential to exploit the vulnerabilities inherent in the design of the system through back-doors; exploitable were hard-coded credentials, an insecure protocol and weak encryption algorithms. Biesecker [54] reported in 2017 that a team of government, industry and academic researchers successfully hacked into a legacy Boeing 757 commercial aircraft, remotely, in a non-laboratory setting, by accessing its systems through radio frequency communications.

4.1. Aerospace and Avionic Systems

Aerospace systems have been subject to increasing degrees of software and hardware integration, implemented through embedded-computing technologies. As a result, the system is plagued with software vulnerabilities, as ensuring that embedded systems are free from security weaknesses is difficult, as explored by Dessiatnikof et al. in [55] and Papp et al. [56]. In [55], the researchers further assert that attacks on aerospace systems can originate from the lower layers, such as the Operating System (OS) kernel, protection mechanisms and context switching as it is difficult, even when formal verification methods are applied, to prove an absence of vulnerabilities within embedded systems. One of the principle conclusions arising from their findings is that attacks against aerospace computer systems can be categorised based on the attacker's skills and aims; the aim is either to corrupt the computing system's core functions or the fault-tolerance mechanisms, such as error detection and recovery systems.

An avionics system provides critical support to crew members and pilots for the safe operation of an aircraft, as it provides weather information, positioning data and communications [57]. Avionics is defined as the combination of aviation with electronics, consisting of embedded systems in aircraft design, development and operation [58]. Avionic systems gather data, such as speed, direction, and air temperature, through external sensors and route appropriate data to other components of the aircraft using an avionic network [59]. In recent times, in a bid to leverage the lower cost of Commercial-Off-The-Shelf (COTS) components and software technologies to provision increased bandwidth and reduce cost, Ethernet networks such as Avionics Full DupleX Switched Ethernet (AFDX)—an IEEE 802.11 protocol-based Wireless Flight Management System (WFMS)—have been used in avionic networks.

Wired avionic communications provide a more secure network with a high degree of reliability and safety, as it is difficult for malicious users to access and inject false data [60,61]. On the other hand, the Avionics Wireless Network (AWN) brings new challenges related to assurance, reliability and security [62,63].

Aircraft avionics not only provide on-board passenger entertainment, but also enable the control of flight functions, navigation, guidance, communications, system operation and monitoring. The high level of integration creates cyber-security concerns, for instance, where Voice-over-the-Radio (VoR) communications are used both with pilots and controllers. The major disadvantages of VoR is the time delay to receive the signal, especially in the case of multiple communications, and the corruption of the signal or ambiguity in understanding between controller and pilot due to noise. The Controller Pilot Data Link (CPDLC), however, is digital and thus more robust to impairments. The air carrier flight operations centres are synchronised with the flight deck to receive the same signal at the same time, allowing maximum risk awareness and informing on the optimum decisions. In recent times, the aviation community has focused on creating a modernised National Airspace System (NAS) underpinned by a new communication system able to improve the interaction between the aircraft and the ground system.

More detail on the attack surfaces across different aerospace and avionic components is provided in the following sub-subsections.

4.1.1. Aircraft Communications Addressing and Reporting System (ACARS)

Aeronautical Radio Incorporated (ARINC) introduced the ACARS data link protocol to reduce crew workload and improve data integrity. ACARS is an ARINC 618-based air-to-ground protocol that transfers data between on-board avionics systems and ground-based ACARS networks [64]. The ACARS system consists of a Control Display Unit (CDU) and ACARS Management Unit (MU); the MU sends and receives digital messages from the ground using existing very high frequency (VHF) radios; on the ground, the system—a network of radio transceivers—receives and transmits data link messages, as well as routing them to various aircraft on the network.

Smith et al. stated in [65,66] that the current use of ACARS by stakeholders extends beyond its original application to serve as flight trackers and the crew automated timekeeping system. The works in [65,66] demonstrate how current ACARS usage systematically breaches location privacy; the authors of [65] showed how sensitive information transmitted over an ACARS wireless channel can lead to a privacy breach for users, supporting a known fact that ACARS messages are susceptible to eavesdropping attacks. The article in [65] was concluded by proposing a privacy framework, and in [66] the use of encryption and policy measures was recommended to arrest known eavesdropping attacks on the communication channel.

4.1.2. Automatic Dependent Surveillance-Broadcast (ADS-B)

Aircraft automatically transmit (ADS-B Out) and/or receive (ADS-B In) identification and positional data in a broadcast mode through a data link using Automatic Dependent Surveillance Broadcast (ADS-B), improving the safety and capacity of airport surveillance and thus enhancing situational awareness of airborne and ground surveillance in airports [67]. Ali et al. [68] state that ADS-B Out provides a range of ground applications support, including Air Traffic Control (ATC) surveillance in both radar and non-radar airspace over the airport, as well as enabling enhanced surveillance applications through links to aircraft in order to receive ADS-B Out messages from other aircraft within their coverage (ADS-B In) areas. The integrity and availability of the ADS-B system is paramount as a result of its role in supporting key ground and airborne applications [69]. Furthermore, Manesh and Kaabouch in [70] stated that ADS-B employing global satellite navigation systems generates precise airspace mappings for air traffic management. Thus, the security of ADS-B has become a major concern as the system broadcasts detailed information about aircraft, their positions, velocities, and other data over unencrypted data links.

Tabassum [71] analysed the performance of ADS-B data received from Grand Fork International Airport. The data were in raw and archived Global Data Link (GDL-90) format. GDL-90 is designed to transmit, receive and decode ADS-B messages through an on-board data link by combining GPS satellite navigation with data link communications. The aim was to detect anomalies in the data and, in turn, quantify the associated risk. In the course of the research, dropout, low-confidence data, message loss, data jump, and altitude discrepancy were identified as anomalies, but the focus was on two of them, dropouts and altitude deviations. The conclusion drawn was that all failures relating to the anomalies have the potential of affecting ATC operation either from an airspace perspective, such as dropout, low-confidence data or from an aircraft perspective, such as data jump, partial message loss and altitude discrepancy. All are surfaces which an attacker can leverage to execute attacks such as eavesdropping, jamming, message injection, deletion and modification [70,72].

4.2. Electronic Flight Bag

The Electronic Flight Bag (EFB) displays digital documentation, such as navigational charts, operations manuals, and airplane checklists by the flight crew. It can also be used by crew members to perform basic flight planning calculations. Advanced EFB now perform many complex flight-planning tasks and are integrated into flight management systems, alongside other avionic systems, to display the real-time position of an aircraft on navigational charts with weather information [57]. Wolf, Minzlaff and Moser [73] assert that EFBs are valuable elements as a replacement of traditional paper references carried on-board as part of the flight management system, thus yielding added benefits by reducing weight. Advanced EFBs integrated into flight management systems, in contrast with the traditional paper-based method that were stand-alone, now present a new attack surface, e.g., a malware-infected EFB will gate denial-of-service attacks to other connected on-board systems [57,73–75].

4.3. Attack Surfaces in the Civil Aviation Industry

Table 4 summarises the range of cyber-attack surfaces identified within the civil aviation industry and recommended ways to mitigate them.

Table 4. Some Exploitable Flaws and Components in the Civil Aviation Industry.

Class	Ref	Component	Mitigation	Description
C,I	[53]	SATCOM terminals	Consistent patching and software updates, phasing out existing legacy encryption as soon as practicable and following current recommendations on the use of cryptographic algorithms and network protocols.	SATCOM terminals can be exploited through some design flaws in areas such as hardcoded credentials, insecure protocol, weak encryption algorithms.
C,I	[55,56]	Aerospace systems	Consistent patching of OS, phasing out existing legacy encryption as soon as practicable and following current recommendations on the use of cryptographic algorithms.	Attackers, based on skill level, can exploit issues with integration of OS in embedded systems, such as in OS kernel, context switching, protection mechanisms.
C,I	[65,66]	ACARS	Phasing out existing legacy encryption as soon as practicable and following current recommendations on the use of cryptographic algorithms and established policy measures.	The ACARS communication channel is susceptible to eavesdropping and privacy breach.
C,I	[71]	ADS-B	Phasing out existing legacy encryption as soon as practicable and following current recommendations on the use of cryptographic algorithms.	The ADS-B communication channel is prone to eavesdropping, jamming attacks, message injection, deletion and modification.
C,I	[62,63]	AWN	Phasing out existing legacy encryption as soon as practicable and following current recommendations on the use of cryptographic algorithms.	The Wireless Avionic Network communication channel is prone to data integrity problems such as data assurance, reliability and security.

Legend: C = Confidentiality, I = Integrity, A = Availability.

5. Mitigation of Cyber-Security Challenges within the Civil Aviation Industry

The mapping of the range of cyber-attacks within the civil aviation industry reveals that phishing and network attacks, such as eavesdropping, DoS, Man-in-the-middle and spoofing attacks, predominate [76]. Distributed Denial-of-Service (DDoS) and DoS attacks on network assets at the airport, most notably, Vulnerability Bandwidth Depletion DDoS Attacks (VBDDA), could be mitigated according to Ugwoke et al. [77] by the proposed embedded Stateful Packet Inspection (SPI) based on the OpenFlow Application Centric Infrastructure (OACI). The focus was to mitigate attacks on Airport Information Resource Management Systems (AIRMS), an enterprise cloud-based resource management system used in some airports. Delain et al. [78] assume a different position on DDoS prevention, adopting volumetric protection through providing an alternative secondary Internet connection, as well as deploying high-performance hardware devices. The latter monitor logging activities and traffic continuously to improve the efficiency of the protection mechanism. Clark and Hakim [79], Martellini [80] and Singer and Friedman [81] propose the use of airport intelligence classification to protect airport assets and infrastructure from cyber-attacks, the method being classified according to good technical practice for high-level security issues. In practice, the approach is founded on a good cyber-hygiene culture, involving system and anti-virus regular updates, cyber-education for new employees, regular data backup and password management. The use of encoding was posited by Efe et al. [52] as a measure to prevent cyber-attacks on ADS-B data used for airborne and ground surveillance in airports. The use of the random blurring technique on aircraft data from ADS-B within permissible error bounds, so as not to impair the operational integrity

of Air Traffic Control (ATC), is also proposed as a means of limiting and monitoring the level of interference of Unmanned Aerial Vehicles (UAVs) on ADS-B data using aircraft information at the airport.

6. The Future Civil Aviation Industry and Its Cyber-Security Challenges

The concept of 'smartness' within the civil aviation industry has its root in the relatively recent deployments embodying the digitalisation of the industry, such as the integration of IoT-enabled devices, sensors into physical systems, the use of blockchain, AI, cloud and big data to sustain the quality of service delivery. The business goal is to provision optimal services, ensuring an enhanced customer experience in a reliable and sustainable manner by targeting the optimisation of growth, operational efficiency, safety and security [10]. The migration to increasing levels of automation through the integration of operational systems spawns new attack surfaces which, in turn, mandates the revision of existing cyber-security implementations, assessment of the ramifications of the new evolving threats, updating both the risk scenario analysis and resilience measures.

6.1. Smart Airports

In addition to the technologies cited under the integrated digital transformation evolution within the airport eco-system, Zamorano et al. in [82] have highlighted other technologies such as Radio Frequency Identification (RFID), geolocation, immersive realities, biometric systems and robotics as core elements within next-generation Smart Airport environments. Koroniotis et al. in [83] are of the view that advances in IoT device integration within the aviation sector infrastructures alone have given rise to the emergence of the Smart Airport. The objective is to deliver an excellent customer experience with improved efficiency in daily operations, enhancing robustness, efficiency and control of service delivery [83]. The acquisition of customer data of interactions with every 'thing' within the airport in real time, as well as its subsequent analyses to generate passenger profiles, is a proven route to gating ancillary revenues [84]. In essence, the Smart Airport is a data-rich environment, equipped with a range of sensors, actuators and other embedded devices that provide customers with a user interface to interact with cyber-physical devices across the environment.

Lykou et al. [10] categorised the scope of threats against IoT infrastructures and applications within smart airports into the following: network and communication attacks, malicious software and tampering with airport smart devices. The scenario analysis of likely malicious attacks also included the misuse of authorisation, social engineering and phishing with consideration of smart applications, mitigating actions and resilience measures. Furthermore, Koroniotis et al. in [83] postulate that IoT systems and devices are prone to APT-led attacks due to hardware constraints, software flaws or misconfigurations. AI-enabled techniques based on machine learning are suggested as a potential methodology to develop solutions that address the challenge of IoT-inspired cyber-attacks. A robust cyber-defence framework in smart airports is of vital importance to ensure the reliability of services and mitigate against service disruptions and cancellations, as well as loss of sensitive information.

6.2. E-Enabled Aircraft

The use of electronic data exchange and digital network connectivity are the spines of the approach adopted by the industry to increase the efficiency of on-board aircraft operations; IoT will play an important role in this respect, according to Wolf et al. [73]. A review on the role and the potential of e-enabled devices in enhancing digital network connectivity and electronic data exchange in future e-enabled aircraft, together with their attendant vulnerabilities, attack surfaces and possible mitigating factors, is thus of benefit.

Mahmoud et al. in 2010 [85] reported on a design of an adaptive security architecture of future network-connected aircraft, while Neumann [86], Sampigethaya et al. [87,88] surveyed both the current and future security provision of embedded system in e-enabled

aircraft networks. Mahmoud et al. [85] proposed a secure system topology for the embedded aircraft system network, referred to as SecMan for application in Fiber-like aircraft satellite telecommunications. Sampigethaya et al. provided evidence that the safety, security and efficiency of e-enabled aircraft will be highly dependent on the security capabilities of the communications, network and cyber-physical systems. The consequence of the deployment of advance sensing, extensive computerised systems, enhanced communication channels between on-ground and on-board systems, on-board system integration and smart software-enabled interfaces is a proliferation of attack surfaces. Such surfaces present opportunities to exploit on-board cyber-physical systems remotely through radio frequency jamming, node impersonation and passive eavesdropping [88]. Table 5 provides a summary of the classes of attacks in the context of the evolution of the sector.

The on-board trend of increasing the degree of integration of IT services into aircraft mechanical devices will undoubtedly enhance efficiencies, however, at the expense of an increase in attack surfaces. The relatively recent harnessing of artificial intelligence techniques by cyber-attackers to automate attack processes [89,90] is a worrying development and stimulates a response strategy also founded on the use of AI-enabled cyber-defence frameworks in safeguarding e-enabled aircraft against severely damaging breaches.

Table 5. A summary of the classes of attacks in next generation aviation systems.

Domain	Ref	Experimental Tests/Scenarios	Tools
IoT	[91]	Network mapping attack/implementation of profiling module (training and testing algorithm)	TestStad/Machine Learning Algorithm
	[92]	Discrete-time Markov chain model (DTMC): Analysing the capacity of the block chain	Block mining algorithm and Ethereum protocol
	[93]	Manual test: Analysis and attacks of each device, Automated test: process testing of different IoT device	Open-Source MS
	[94]	DoS massif traffic/Transfer Data/Abnormal code/System crash	DTM by Triangle Micro Works
	[95]	Real-world attack scenarios: internal and external network attacks	SDN/network function virtualisation
	[96]	Anomaly intrusion/attacks traffic	Machine learning algorithm/feature extraction
	[97]	Command injection attack	Machine learning algorithm/PLC programming by Ladder language
	[98]	SWaT/WADI datasets: Normal and attack scenario	Machine learning algorithm
	[99]	Man-in-the-middle attack	SDN /Python
	[100]	LAUP algorithm(authentication)/key distribution test	COOJA simulator
Smart Grid	[101]	Offline co-simulation Test-bed: DoS/FDI attacks	OMNET++
	[102]	Access to communication link ([103]) attack model	OPAL-RT
	[104]	Deep packet inspection	Software-Defined Networks/OpenFMB
	[105]	Power supply interruption Attack/Physical damage attack	Real world power system/Machine learning
	[106]	MMS/GOOSE/SV implementation	IEC 61850 Protocol/Ethernet RaspberryPi 3B+

Table 5. *Cont.*

Domain	Ref	Experimental Tests/Scenarios	Tools
	[107]	HIL simulation/proof-of-concept validation	Python
	[108]	DoS/Man in the middle attacks/TCP SYN Flood Attack	DeterLab/Security Experimentation EnviRonment (SEER)
	[109]	Recording network traffic/poisoning attack	Real-Time Digital Simulator (RTDS)
	[110]	Timing Intrusion Attack	Field End-to-End Calibrator/Gold PMU
	[111]	Test of cyber-physical sensor: IREST	Idaho CPS SCADA Cybersecurity (ISAAC) testbed
	[112]	MITM attack/DoS attack	Open-source software/Raspberry Pis. FLEP-SGS
Cloud	[113]	Flood malicious traffic (ICMP/HTTP/SYN)	VMware Esxi hypervisor/A vCenter server/VMs
	[114]	Considering small messages (about1–2 KBytes): Fast filling of the buffers	MOM4Cloud architectural model.
	[115]	UNM database: Malicious tracing logs	KVM2.6.27 hypervisor/Python3.4
	[116]	Test of memory usage before or after instance creation	OpenStack: Open-Source cloud operating system
	[117]	Evaluation of performance metrics of NDN/edge cloud computing	Cloud VM
	[118]	Adding defaults: broken interconnection/abnormal extruder	MTComm: Online Machine Tool Communication
	[119]	Side-channel attacks/stealthy data exfiltration	DHCP server/TFTP Server/HTTP Server/MQTT Server
	[120]	SQL Injection attack	OpenStack implementation/Python
	[121]	Testing traffic scenarios	Openflow controller/OpenvSwitch/Network virtualization agent
	[122]	Time-inference attacks	Software-Defined Network
	[123]	DDoS attack	OpenStack environment

7. Conclusions

The review presented a mapping of the cyber-attack incidents within the civil aviation industry over the last 20 years, through a search of the published literature and documented cyber-attacks, as well as capturing the motives of the threat actors. Results show that the main cyber-threat to the industry stem from APT groups, in collaboration with state actors, the goal being to acquire intellectual property and intelligence in order to advance domestic aerospace capabilities as well as monitor, infiltrate and subvert other nations' capabilities.

As is the obligation of any industry, the aviation sector continues to strive to improve the quality of services provided and enhance customer experience. The approach followed to satisfy the business need is founded on increasing the levels of system integration, the judicious embedding of automation where appropriate and an increase in the use of data. The evolution to date has been seeded through the implementation of IoT technologies, not only to increase the level of inter-connectivity on-ground, on-board and between the two domains, but also to gather key sensor and customer behaviour data, the former necessary to optimise on-board (e-aircraft) operations, whilst the latter—to enhance on-ground (smart airport) customer experience. However, the higher levels of integration and connectivity spawn a spectrum of new cyber-attack surfaces and, given the ability of attackers to automate attack processes through AI, there is an immediate need to develop holistic cyber-defence strategies to protect the cyber-integrity of the emerging Smart Airport and e-enabled aircraft systems. Otherwise, there exists a great likelihood that APT groups could advance beyond attacking airport facilities only to breach on-board and in-flight aircraft by using sophisticated remote attack tools with severe concomitant damages and loss of life.

8. Open Challenges and Research Opportunities

The combination of digital transformation, connectivity, segmentation and complexity currently being experienced in the industry due to the surge in global travel will continue to pose challenges in terms of cyber-security. The increasing levels of integration and automation to satisfy the needs of the business exposes the sector by presenting new opportunities for cyber-attacks. There is no doubt that the evolution will improve the quality of services provided and improve the customer experience but at the expense of exposing new attack surfaces to cyber-threat actors, which will stimulate a proliferation in the number of attacks. Furthermore, the industry is also obligated to protect legacy IT infrastructures and entrenched practices exacerbated further by the fragmentation in the industry, which increases the complexity of the challenge, as much of the systems in use were not designed to be robust against cyber-crime.

In this context, the difficulty of securing accurate information of sufficient scope on the nature and magnitude of cyber-incidents within the industry remains an open challenge that hinders innovation. News channels, blogs or company websites provide minimal information on cyber-breaches due to the sensitive nature of the industry and its dominance by government-owned agencies. This practice, whilst understandable from an industry perspective, presents researchers with challenges in developing fit-for-purpose solutions that support the evolution of the sector. Developers thus resort to performing informed quantitative analysis of potentially skewed data to reach meaningful conclusions.

Thus, clearly evident are the emerging opportunities for the development of AI-based cyber-security solutions that address the major threats to the operational integrity of the aviation industry. Innovating proactive, offence-centric measures for the protection of avionic infrastructures characterised by increasing levels of automation and, in turn, creating additional attack surfaces, presents a rich vein of opportunities.

Author Contributions: Conceptualization, E.U., M.A.B.-F., H.H. and X.B.; investigation, E.U. and H.H.; methodology, E.U., X.B. and H.H.; administration, X.B. and I.A.; supervision, X.B. and I.A.; validation, M.B., E.U., R.A., C.T., X.B. and I.A.; writing—original draft preparation, E.U. and H.H.; writing—review and editing, M.B., E.U., H.H., M.A.B.-F., R.A., C.T., X.B. and I.A. All authors have read and agreed to the published version of the manuscript.

Funding: The research is supported by the European Union Horizon 2020 Programme "FORESIGHT (Advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments)" under Grant Agreement No. 833673. The content reflects the authors' view only and the Agency is not responsible for any use that may be made of the information within the paper.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: All data analysed and used in this paper are secondary and publicly available data.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Duchamp, H.; Bayram, I.; Korhani, R. Cyber-Security, a new challenge for the aviation and automotive industries. In *Seminar in Information Systems: Applied Cybersecurity Strategy for Managers*; 2016; pp. 1–4. Available online: https://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf (accessed on 20 September 2020).
2. Monteagudo, J. Aviation Cybersecurity—High Level Analysis, Major Challenges and Where the Industry Is Heading. 2020. Available online: https://cyberstartupobservatory.com/aviation-cybersecurity-major-challenges/ (accessed on 26 September 2020).
3. Bellekens, X.; Jayasekara, G.; Hindy, H.; Bures, M.; Brosset, D.; Tachtatzis, C.; Atkinson, R. From cyber-security deception to manipulation and gratification through gamification. In *International Conference on Human-Computer Interaction*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 99–114.
4. ICAO. Security and Facilitation Strategic Objective: Aviation Cybersecurity Strategy. 2019. Available online: https://www.icao.int/cybersecurity/Documents/AVIATIONCYBERSECURITYSTRATEGY.EN.pdf (accessed on 6 December 2021).

5. Okoli, C.; Schabram, K. A Guide to Conducting a Systematic Literature Review of Information Systems Research. 2010. Available online: https://asset-pdf.scinapse.io/prod/1539987097/1539987097.pdf (accessed on 6 December 2021).
6. Okoli, C. A Guide to Conducting a Standalone Systematic Literature Review. 2015. Available online: https://aisel.aisnet.org/cais/vol37/iss1/43/ (accessed on 6 December 2021).
7. IATA. Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation. 2020. Available online: https://www.iata.org/contentassets/4c51b00fb25e4b60b38376a4935e278b/compilationofcyberregulationsstandardsandguidanceapr212.0.pdf (accessed on 6 December 2021).
8. Haass, J.; Sampigethaya, R.; Capezzuto, V. Aviation and cybersecurity: Opportunities for applied research. *TR News* **2016**, *304*, 39.
9. Lykou, G.; Anagnostopoulou, A.; Gritzalis, D. Implementing cyber-security measures in airports to improve cyber-resilience. In Proceedings of the 2018 Global Internet of Things Summit (GIoTS), Bilbao, Spain, 4–7 June 2018; pp. 1–6.
10. Lykou, G.; Anagnostopoulou, A.; Gritzalis, D. Smart airport cybersecurity: Threat mitigation and cyber resilience controls. *Sensors* **2019**, *19*, 19. [CrossRef] [PubMed]
11. Gopalakrishnan, K.; Govindarasu, M.; Jacobson, D.W.; Phares, B.M. Cyber security for airports. *Int. J. Traffic Transp. Eng.* **2013**, *3*, 365–376. [CrossRef]
12. Mathew, A.R. Airport Cyber Security and Cyber Resilience Controls. *arXiv* **2019**, arXiv:1908.09894.
13. Suciu, G.; Scheianu, A.; Vulpe, A.; Petre, I.; Suciu, V. Cyber-attacks–The impact over airports security and prevention modalities. In *World Conference on Information Systems and Technologies*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 154–162.
14. Corretjer, P.J. A Cybersecurity Analysis of Today's Commercial Aircrafts and Aviation Industry Systems. Master's Thesis, Utica College, Utica, NY, USA, 2018; p. 22.
15. Kagalwalla, N.; Churi, P.P. Cybersecurity in Aviation: An Intrinsic Review. In Proceedings of the 2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA), Pune, India, 19–21 September 2019; pp. 1–6.
16. Lehto, M. Cyber Security in Aviation, Maritime and Automotive. In *Computation and Big Data for Transport*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 19–32.
17. CyberRisk, I. Cyber Threats to the Aviation Industry. 2020. Available online: https://cyberriskinternational.com/2020/04/06/cyber-threats-to-the-aviation-industry/ (accessed on 19 September 2020).
18. Fireeye. Cyber Threats to the Aerospace and Defense Industries. 2016. Available online: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf (accessed on 24 September 2020).
19. Varonis. 9 Infamous APT Groups: Fast Fact Trading Cards. 2020. Available online: https://www.varonis.com/blog/apt-groups (accessed on 6 December 2021).
20. Kessler, G.C.; Craiger, J.P. Aviation Cybersecurity: An Overview. 2018. Available online: https://commons.erau.edu/ntas/2018/presentations/37/ (accessed on 6 December 2021).
21. Abeyratne, R. Aviation and Cybersecurity in the Digital World. In *Aviation in the Digital Age*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 173–211.
22. Arampatzis, A. The State of Civil Aviation Cybersecurity. 2020. Available online: https://www.tripwire.com/state-of-security/security-data-protection/civil-aviation-cybersecurity/ (accessed on 30 September 2020).
23. Viveros, C.A.P. Analysis of the Cyber Attacks against ADS-B Perspective of Aviation Experts. Master's Thesis, University of Tartu, Tartu, Estonia, 2016.
24. Gross, G. FAA: Slammer Didn't Hurt Us, but Other Attacks Coming. 2003. Available online: https://www.networkworld.com/article/2339600/faa--slammer-didn-t-hurt-us--but-other-attacks-coming.html (accessed on 19 September 2020).
25. Goodin, D. US Air Traffic Faces 'Serious Harm' from Cyber Attackers. 2009. Available online: Https://www.theregister.com/2009/05/07/air-traffic-cyber-attack/ (accessed on 19 September 2020).
26. Ellinor, M. Report: Hackers Broke into FAA Air Traffic Control Systems. 2009. Available online: https://www.cnet.com/tech/services-and-software/report-hackers-broke-into-faa-air-traffic-control-systems/ (accessed on 19 September 2020).
27. Paganini, P. Istanbul Ataturk International Airport Targeted by a Cyber-Attack. 2013. Available online: https://securityaffairs.co/wordpress/16721/hacking/istanbul-ataturk-international-airport-targeted-by-cyber-attack.html (accessed on 19 September 2020).
28. Welsh, W. Phishing Scam Targeted 75 US Airports. 2014. Available online: https://www.informationweek.com/?1 (accessed on 19 September 2020).
29. Brewster, T. Attack On LOT Polish Airline Grounds 10 Flights. 2015. Available online: https://www.forbes.com/sites/thomasbrewster/2015/06/22/lot-airline-hacked/?sh=6e4015fe124e (accessed on 19 September 2020).
30. Kirkliauskaite, K. Main Cyber-Security Challenges in Aviation. 2020. Available online: https://www.aerotime.aero/25150-main-cyber-security-challenges-in-aviation (accessed on 19 September 2020).
31. Polityuk, P.; Prentice, A. Ukraine Says to Review Cyber Defenses after Airport Targeted from Russia. 2016. Available online: https://www.reuters.com/article/us-ukraine-cybersecurity-malware-idUSKCN0UW0R0 (accessed on 6 October 2020).
32. Park, K. Cathay Pacific Cyber Attack Is World's Biggest Airline Data Breach. 2018. Available online: https://www.insurancejournal.com/news/international/2018/10/26/505699.html (accessed on 19 September 2020).
33. Sandle, P. British Airways Says 'Sophisticated' Hacker Stole Data on 380,000 Customers. 2018. Available online: https://www.insurancejournal.com/news/international/2018/09/10/500566.htm (accessed on 19 September 2020).

34. Singh, K. Delta, Sears Report Data Breach by Service Provider. 2018. Available online: https://www.insurancejournal.com/news/national/2018/04/05/485440.htm (accessed on 19 September 2020).
35. Leyden, J. Brit Airport Pulls Flight info System Offline after Attack by 'Online Crims'. 2018. Available online: https://www.theregister.com/2018/09/17/bristol-airport-cyber-attack/ (accessed on 19 September 2020).
36. Sandle, T. Air Canada Suffers Major App Data Breach of 20,000 Customers. 2018. Available online: https://www.digitaljournal.com/business/air-canada-in-major-app-data-breach/article/530763 (accessed on 19 September 2020).
37. Gibbs, B. Potential Personally Identifiable Information (PII) Compromise of NASA Servers. 2018. Available online: Http://spaceref.com/news/viewsr.html?pid=52074/ (accessed on 22 September 2020).
38. Gates, D. Boeing Hit by WannaCry Virus, but Says Attack Caused Little Damage. 2018. Available online: https://www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/ (accessed on 22 September 2020).
39. Solomon, S. Israeli Airports Fend Off 3 Million Attempted Attacks a Day, Cyber Head Says. 2019. Available online: https://www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (accessed on 19 September 2020).
40. Duvelleroy, M. Airbus Statement on Cyber Incident. 2019. Available online: https://www.airbus.com/en/newsroom/press-releases/2019-01-airbus-statement-on-cyber-incident (accessed on 22 September 2020).
41. Goud, N. Ransomware Attack on Albany Airport on Christmas 2019. 2019. Available online: https://www.cybersecurity-insiders.com/ransomware-attack-on-albany-airport-on-christmas-2019/ (accessed on 25 September 2020).
42. Team, N. Cryptocurrency Miners Infected More than 50% of the European Airport Workstations. 2019. Available online: https://www.cyberdefensemagazine.com/cryptocurrency-miners-infected-more-than-50-of-the-european-airport-workstations/ (accessed on 25 September 2020).
43. Narendra, M. Privacy: Air New Zealand Experiences Data Breach. 2019. Available online: https://www.grcworldforums.com/news/2019/08/16/privacy-air-new-zealand-experiences-data-breach/ (accessed on 25 September 2020).
44. Montalbano, E. DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla. 2020. Available online: https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/ (accessed on 22 September 2020).
45. Chua, A. Ransomware Attack hits ST Engineering's USA Aerospace Unit. 2020. Available online: https://www.flightglobal.com/aerospace/ransomware-attack-hits-st-engineerings-usa-aerospace-unit/138722.article (accessed on 23 September 2020).
46. Claburn, T. Airline Software Super-Bug: Flight Loads Miscalculated Because Women Using 'Miss' Were Treated as Children. 2021. Available online: https://www.theregister.com/2021/04/08/tuisoftwaremistake/ (accessed on 9 April 2021).
47. Mazareanu, E. Number of Public and Private Airports in the United States from 1990 to 2019*. 2020. Available online: https://www.statista.com/statistics/183496/number-of-airports-in-the-united-states-since-1990/ (accessed on 28 November 2020).
48. Paganini, P. Cyber Threats against the Aviation Industry. 2014. Available online: https://resources.infosecinstitute.com/topic/cyber-threats/ (accessed on 19 September 2020).
49. Thales. Overcoming the Cyber Threat in Aviation. 2016. Available online: https://onboard.thalesgroup.com/overcoming-cyber-threat-aviation/ (accessed on 24 September 2020).
50. Zetter, K. Feds Say that Banned Researcher Commandeered a Plane. 2015. Available online: https://www.wired.com/2015/05/ (accessed on 18 January 2022).
51. Freiherr, G. Will Your Airliner Get Hacked? 2021. Available online: https://www.smithsonianmag.com/air-space-magazine/will-your-airliner-get-hacked-180976752/ (accessed on 18 January 2022).
52. Efe, A.; Tuzlupınar, B.; Cavlan, A.C. Air Traffic Security against Cyber Threats. *Bilge Int. J. Sci. Technol. Res.* **2021**, *3*, 135–143. Available online: https://dergipark.org.tr/en/pub/bilgesci/issue/49118/405074 (accessed on 18 January 2021).
53. Santamarta, R. A Wake-Up Call for SATCOM Security. Technical White Paper. 2014. Available online: https://www.secnews.gr/wp-content/uploads/Files/Satcom_Security.pdf (accessed on 19 September 2020).
54. Biesecker, C. *Boeing 757 Testing Shows Airplanes Vulnerable to Hacking, DHS Says*; Avionics International: New York, NY, USA, 2017
55. Dessiatnikoff, A.; Deswarte, Y.; Alata, E.; Nicomette, V. Potential attacks on onboard aerospace systems. *IEEE Secur. Priv.* **2012**, *10*, 71–74. [CrossRef]
56. Papp, D.; Ma, Z.; Buttyan, L. Embedded systems security: Threats, vulnerabilities, and attack taxonomy. In Proceedings of the 2015 13th Annual Conference on Privacy, Security and Trust (PST), Izmir, Turkey, 21–23 July 2015; pp. 145–152.
57. GAO. Aviation Cybersecurity. 2020. Available online: https://www.gao.gov/assets/gao-21-86.pdf (accessed on 12 May 2020).
58. *Encyclopedia of Physical Science and Technology*; Academic Press: Cambridge, MA, USA, 1987.
59. Smith, B. System and Method for Data Collection in an Avionics Network. U.S. Patent App. 11/092,470, 28 September 2006.
60. Akram, R.N.; Markantonakis, K.; Holloway, R.; Kariyawasam, S.; Ayub, S.; Seeam, A.; Atkinson, R. Challenges of security and trust in avionics wireless networks. In Proceedings of the 2015 IEEE/AIAA 34th Digital Avionics Systems Conference (DASC), Prague, Czech Republic, 13–17 September 2015; pp. 777–780.
61. Akram, R.N.; Markantonakis, K.; Mayes, K.; Bonnefoi, P.F.; Sauveron, D.; Chaumette, S. An efficient, secure and trusted channel protocol for avionics wireless networks. In Proceedings of the 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 25–29 September 2016; pp. 1–10.

62. Akram, R.N.; Markantonakis, K.; Mayes, K.; Bonnefoi, P.F.; Sauveron, D.; Chaumette, S. Security and performance comparison of different secure channel protocols for Avionics Wireless Networks. In Proceedings of the 2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC), Sacramento, CA, USA, 25–29 September 2016; pp. 1–8.
63. Markantonakis, K.; Akram, R.N.; Holloway, R. A secure and trusted boot process for avionics wireless networks. In Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, USA, 19–21 April 2016; pp. 1C3-1–1C3-9.
64. Bellamy, W., III. How ACARS Will Evolve, Not Disappear, With Transition to IPS. 2018. Available online: https://www.aviationtoday.com/2018/06/12/acars-will-evolve-not-disappear-transition-ips/ (accessed on 28 September 2020).
65. Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I. Analyzing privacy breaches in the aircraft communications addressing and reporting system (acars). *arXiv* **2017**, arXiv:1705.07065.
66. Smith, M.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I. Undermining privacy in the aircraft communications addressing and reporting system (ACARS). *Proc. Priv. Enhancing Technol.* **2018**, *2018*, 105–122. [CrossRef]
67. Ali, B.S. A Safety Assessment Framework for Automatic Dependent Surveillance Broadcast (ADS-B) and Its Potential Impact on Aviation Safety. Ph.D. Thesis, Centre for Transport Studies, Department of Civil and Environmental, Imperial College London, London, UK, 2013.
68. Ali, B.S.; Schuster, W.; Ochieng, W.Y. Evaluation of the capability of automatic dependent surveillance broadcast to meet the requirements of future airborne surveillance applications. *J. Navig.* **2017**, *70*, 49. [CrossRef]
69. Ali, B.S.; Ochieng, W.Y.; Schuster, W.; Majumdar, A.; Chiew, T.K. A safety assessment framework for the Automatic Dependent Surveillance Broadcast (ADS-B) system. *Saf. Sci.* **2015**, *78*, 91–100. [CrossRef]
70. Manesh, M.R.; Kaabouch, N. Analysis of vulnerabilities, attacks, countermeasures and overall risk of the Automatic Dependent Surveillance-Broadcast (ADS-B) system. *Int. J. Crit. Infrastruct. Prot.* **2017**, *19*, 16–31. [CrossRef]
71. Tabassum, A. Performance Analysis of Automatic Dependent Surveillance-Broadcast (ADS-B) and Breakdown of Anomalies. 2017. Available online: https://www.proquest.com/openview/8e29fdfcd2afbe8ce28f760d0a314248/1?pq-origsite=gscholar&cbl=18750 (accessed on 28 September 2020).
72. Strohmeier, M.; Lenders, V.; Martinovic, I. On the security of the automatic dependent surveillance-broadcast protocol. *IEEE Commun. Surv. Tutor.* **2014**, *17*, 1066–1087. [CrossRef]
73. Wolf, M.; Minzlaff, M.; Moser, M. Information technology security threats to modern e-enabled aircraft: A cautionary note. *J. Aerosp. Inf. Syst.* **2014**, *11*, 447–457. [CrossRef]
74. Howard, E. Dell and Airbus deliver Electronic Flight Bag Services to Airlines Worldwide. 2013. Available online: https://www.intelligent-aerospace.com/commercial/article/16539972/dell-and-airbus-deliver-electronic-flight-bag-services-to-airlines-worldwide (accessed on 12 February 2021).
75. Keller, J. Fokker Services Certifies iPad Electronic Flight Bag (EFB) for Bombardier Dash 8 Twin-Engine Passenger Turboprop. 2013. Available online: https://www.intelligent-aerospace.com/commercial/article/16539248/fokker-services-certifies-ipad-electronic-flight-bag-efb-for-bombardier-dash-8-twinengine-passenger-turboprop (accessed on 12 February 2021).
76. Taleqani, A.R.; Nygard, K.E.; Bridgelall, R.; Hough, J. Machine Learning Approach to Cyber Security in Aviation. In Proceedings of the 2018 IEEE International Conference on Electro/Information Technology (EIT), Rochester, MI, USA, 3–5 May 2018; pp. 0147–0152.
77. Ugwoke, F.; Okafor, K.; Chijindu, V. Security QoS profiling against cyber terrorism in airport network systems. In Proceedings of the 2015 International Conference on Cyberspace (CYBER-Abuja), Abuja, Nigeria, 4–7 November 2015; pp. 241–251.
78. Delain, O.; Ruhlmann, O.; Vautier, E.; Johnson, C.; Shreeve, M.; Sirko, P.; Prozserin, V. Cyber-Security Application for SESAR OFA 05.01.01—Final Report. 2016. Available online: https://www.sesarju.eu/sites/default/files/documents/news/AddressingairportcybersecurityFull0.pdf (accessed on 3 April 2020).
79. Clark, R.M.; Hakim, S. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*; Springer: Berlin/Heidelberg, Germany, 2016; Volume 3.
80. Martellini, M. *Cyber Security: Deterrence and IT Protection for Critical Infrastructures*; Springer: Berlin/Heidelberg, Germany, 2013.
81. Singer, P.W.; Friedman, A. *Cybersecurity: What Everyone Needs to Know*; OUP USA: New York, NY, USA, 2014.
82. Zamorano, M.M.; Fernández-Laso, M.C.; de Esteban Curiel, J. Smart Airports: Acceptance of Technology by Passengers. *Cuad. Tur.* **2020**, *45*, 567–570.
83. Koroniotis, N.; Moustafa, N.; Schiliro, F.; Gauravaram, P.; Janicke, H. A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *IEEE Access* **2020**, *8*, 209802–209834. [CrossRef]
84. Akar, I.N.; Yaqoobi, M.H. Smart Airport: How IOT and New Technologies Shaping the Future of Airport Industry. Available online: https://hadiyaqoobi.github.io/Graduation-project/documents/Thesis202.1.pdf (accessed on 3 April 2020).
85. Mahmoud, M.S.B.; Larrieu, N.; Pirovano, A.; Varet, A. An adaptive security architecture for future aircraft communications. In Proceedings of the 29th Digital Avionics Systems Conference, Salt Lake City, UT, USA, 3–7 October 2010; pp. 3.E.2-1–3.E.2-16. [CrossRef]
86. Neumann, P.G. Computer security in aviation: Vulnerabilities, threats, and risks. In *International Conference on Aviation Safety in the 21st Century*; White House Commission on Safety and Security and George Washington University: Washington, DC, USA, 1997.
87. Sampigethaya, K.; Poovendran, R.; Bushnell, L. Secure operation, control, and maintenance of future e-enabled airplanes. *Proc. IEEE* **2008**, *96*, 1992–2007. [CrossRef]

88. Sampigethaya, K.; Poovendran, R.; Shetty, S.; Davis, T.; Royalty, C. Future e-enabled aircraft communications and security: The next 20 years and beyond. *Proc. IEEE* **2011**, *99*, 2040–2055. [CrossRef]
89. Kaloudi, N.; Li, J. The ai-based cyber threat landscape: A survey. *ACM Comput. Surv. (CSUR)* **2020**, *53*, 1–34. [CrossRef]
90. Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; et al. The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv* **2018**, arXiv:1802.07228.
91. Siboni, S.; Sachidananda, V.; Shabtai, A.; Elovici, Y. Security Testbed for the Internet of Things. *arXiv* **2016**, arXiv:1610.05971.
92. Wang, X.; Yu, G.; Zha, X.; Ni, W.; Liu, R.P.; Guo, Y.J.; Zheng, K.; Niu, X. Capacity of blockchain based internet-of-things: Testbed and analysis. *Internet Things* **2019**, *8*, 100109. [CrossRef]
93. Waraga, O.A.; Bettayeb, M.; Nasir, Q.; Talib, M.A. Design and implementation of automated IoT security testbed. *Comput. Secur.* **2020**, *88*, 101648. [CrossRef]
94. Lee, S.; Lee, S.; Yoo, H.; Kwon, S.; Shon, T. Design and implementation of cybersecurity testbed for industrial IoT systems. *J. Supercomput.* **2018**, *74*, 4506–4520. [CrossRef]
95. Kim, Y.; Nam, J.; Park, T.; Scott-Hayward, S.; Shin, S. SODA: A software-defined security framework for IoT environments. *Comput. Netw.* **2019**, *163*, 106889. [CrossRef]
96. Shafiq, M.; Tian, Z.; Sun, Y.; Du, X.; Guizani, M. Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city. *Future Gener. Comput. Syst.* **2020**, *107*, 433–442. [CrossRef]
97. Zolanvari, M.; Teixeira, M.A.; Jain, R. Effect of imbalanced datasets on security of industrial IoT using machine learning. In Proceedings of the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), Miami, FL, USA, 9–11 November 2018; pp. 112–117.
98. Elnour, M.; Meskin, N.; Khan, K.; Jain, R. A Dual-Isolation-Forests-Based Attack Detection Framework for Industrial Control Systems. *IEEE Access* **2020**, *8*, 36639–36651. [CrossRef]
99. Molina Zarca, A.; Bernal Bernabe, J.; Farris, I.; Khettab, Y.; Taleb, T.; Skarmeta, A. Enhancing IoT security through network softwarization and virtual security appliances. *Int. J. Netw. Manag.* **2018**, *28*, e2038. [CrossRef]
100. Arockia Baskaran, A.G.R.; Nanda, P.; Nepal, S.; He, S. Testbed evaluation of Lightweight Authentication Protocol (LAUP) for 6LoWPAN wireless sensor networks. *Concurr. Comput. Pract. Exp.* **2019**, *31*, e4868. [CrossRef]
101. Hammad, E.; Ezeme, M.; Farraj, A. Implementation and development of an offline co-simulation testbed for studies of power systems cyber security and control verification. *Int. J. Electr. Power Energy Syst.* **2019**, *104*, 817–826. [CrossRef]
102. Poudel, S.; Ni, Z.; Malla, N. Real-time cyber physical system testbed for power system security and control. *Int. J. Electr. Power Energy Syst.* **2017**, *90*, 124–133. [CrossRef]
103. Hahn, A.; Ashok, A.; Sridhar, S.; Govindarasu, M. Cyber-physical security testbeds: Architecture, application, and evaluation for smart grid. *IEEE Trans. Smart Grid* **2013**, *4*, 847–855. [CrossRef]
104. De La Torre, G.; Rad, P.; Choo, K.K.R. Implementation of deep packet inspection in smart grids and industrial Internet of Things: Challenges and opportunities. *J. Netw. Comput. Appl.* **2019**, *135*, 32–46. [CrossRef]
105. Adepu, S.; Kandasamy, N.K.; Mathur, A. Epic: An electric power testbed for research and training in cyber physical systems security. In *Computer Security*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 37–52.
106. Fujdiak, R.; Blazek, P.; Chmelar, P.; Dittrich, P.; Voznak, M.; Mlynek, P.; Slacik, J.; Musil, P.; Jurka, P.; Misurec, J. Communication Model of Smart Substation for Cyber-Detection Systems. In *International Conference on Computer Networks*; Springer: Berlin/Heidelberg, Germany, 2019; pp. 256–271.
107. Cheng, Z.; Chow, M.Y. The Development and Application of a DC Microgrid Testbed for Distributed Microgrid Energy Management System. In Proceedings of the IECON 2018-44th Annual Conference of the IEEE Industrial Electronics Society, Washington, DC, USA, 21–23 October 2018; pp. 300–305.
108. Liu, R.; Srivastava, A. Integrated simulation to analyze the impact of cyber-attacks on the power grid. In Proceedings of the 2015 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES), Seattle, WA, USA, 13 April 2015; pp. 1–6.
109. Oyewumi, I.A.; Jillepalli, A.A.; Richardson, P.; Ashrafuzzaman, M.; Johnson, B.K.; Chakhchoukh, Y.; Haney, M.A.; Sheldon, F.T.; de Leon, D.C. ISAAC: The idaho CPS smart grid cybersecurity testbed. In Proceedings of the 2019 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 7–8 February 2019; pp. 1–6.
110. Kezunovic, M.; Qian, C.; Seidl, C.; Ren, J. Testbed for Timing Intrusion Evaluation and Tools for Lab and Field Testing of Synchrophasor System. In Proceedings of the 2019 International Conference on Smart Grid Synchronized Measurements and Analytics (SGSMA), College Station, TX, USA, 21–23 May 2019; pp. 1–8.
111. Marino, D.L.; Wickramasinghe, C.S.; Amarasinghe, K.; Challa, H.; Richardson, P.; Jillepalli, A.A.; Johnson, B.K.; Rieger, C.; Manic, M. Cyber and Physical Anomaly Detection in Smart-Grids. *IEEE Resil. Week (RWS)* **2019**, *2019*, 187–193. [CrossRef]
112. Konstantinou, C.; Sazos, M.; Maniatakos, M. FLEP-SGS 2: A Flexible and Low-cost Evaluation Platform for Smart Grid Systems Security. In Proceedings of the 2019 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 18–21 February 2019; pp. 1–5.
113. Patil, R.; Dudeja, H.; Modi, C. Designing an efficient security framework for detecting intrusions in virtual network of cloud computing. *Comput. Secur.* **2019**, *85*, 402–422. [CrossRef]
114. Celesti, A.; Fazio, M.; Galletta, A.; Carnevale, L.; Wan, J.; Villari, M. An approach for the secure management of hybrid cloud–edge environments. *Future Gener. Comput. Syst.* **2019**, *90*, 1–19. [CrossRef]

115. Mishra, P.; Verma, I.; Gupta, S. KVMInspector: KVM Based introspection approach to detect malware in cloud environment. *J. Inf. Secur. Appl.* **2020**, *51*, 102460. [CrossRef]
116. Van, V.N.; Chi, L.M.; Long, N.Q.; Nguyen, G.N.; Le, D.N. A performance analysis of openstack open-source solution for IaaS cloud computing. In *Proceedings of the Second International Conference on Computer and Communication Technologies*; Springer: Berlin/Heidelberg, Germany, 2016; pp. 141–150.
117. Ullah, R.; Rehman, M.A.U.; Kim, B.S. Design and Implementation of an Open Source Framework and Prototype for Named Data Networking-Based Edge Cloud Computing System. *IEEE Access* **2019**, *7*, 57741–57759. [CrossRef]
118. Al Sunny, S.N.; Liu, X.; Shahriar, M.R. Remote Monitoring and Online Testing of Machine Tools for Fault Diagnosis and Maintenance Using MTComm in a Cyber-Physical Manufacturing Cloud. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 532–539.
119. Sanatinia, A.; Deshpande, S.; Munshi, A.; Kohlbrenner, D.; Yessaillian, M.; Symonds, S.; Chan, A.; Noubir, G. Hyperdrive: A flexible cloud testbed for research and education. In Proceedings of the 2017 IEEE International Symposium on Technologies for Homeland Security (HST), Waltham, MA, USA, 25–26 April 2017; pp. 1–4.
120. Frank, M.; Leitner, M.; Pahi, T. Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. In Proceedings of the 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), Orlando, FL, USA, 6–10 November 2017; pp. 38–46.
121. Gao, H.; Peng, Y.; Jia, K.; Wen, Z.; Li, H. Cyber-physical systems testbed based on cloud computing and software defined network. In Proceedings of the 2015 International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), Adelaide, SA, Australia, 23–25 September 2015; pp. 337–340.
122. Khorsandroo, S.; Tosun, A.S. Time Inference Attacks on Software Defined Networks: Challenges and Countermeasures. In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2–7 July 2018; pp. 342–349.
123. Kalliola, A.; Lal, S.; Ahola, K.; Oliver, I.; Miche, Y.; Holtmanns, S. Testbed for security orchestration in a network function virtualization environment. In Proceedings of the 2017 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Berlin, Germany, 6–8 November 2017; pp. 1–4.