CYBER SECURITY IN CIVIL AVIATION: CURRENT TRENDS

Prof. (Dr.) Kanwal DP Singh[1]
Dr. Jitender Loura[2]

Abstract

Aviation industry is growing at an ever-fast pace in terms of the growth in number of passengers, regular innovations and technological changes, the growing revenue stream, and the enhanced cyber-threats that come with this growth. For this reason the terms aviation and cyber security are almost used together. The recent changes in technology have made it necessary to focus on different measures of cyber security in the stream of aviation industry, particularly in its three pillars of ATC, airlines, and airports. Theindustry stakeholders necessitates that a serious effort be made in safeguarding the aviation industry from Cyber-attacks.

The use of technologies like Block chain, IoT and AI etc. are highlighted in context of airports being revamped for securing the data being shared and for enhancing the customer experience. The latter is because of the focus on tapping the revenue stream that is being promised due to increased passengers. A focus has been laid on Indian context, while discussing the international aspects as well. In order to show the efforts made to safeguard and criminalize the malicious acts in aviation industry, the discussion also sheds light on the various regulatory measures being applied in the nation. The attempt here is to shed a light on the recent trends and the goals of the nation to both safeguard this industry and to use the growing revenue stream for its advantage.

Key words

Cyber-Security, Civil Aviation, Airlines, Airports, Air Traffic Control, Block Chain

I. INTRODUCTION

India has the second-highest client-based Internet in the world in its emerging digital economy. Lead practices of the Union government such as 'Internet India' and the focus on digital based governance are raising the data structure of the world.[3] In future, integrity in the cyber networks of India will be increasingly challenged and fragile. The Indian aviation industry is the fastest growing industry in the country. Following

[1]Professor & Former Dean, University School of Law and Legal Studies (USLLS), Guru Gobind Singh Indraprastha University, Delhi-110078, India. Email: Kanwal.als@gmail.com

[2]Dy. Director, Directorate General of Civil Aviation (DGCA), Ministry of Civil Aviation, Govt.of India and Research Scholar, USLLS, Guru Gobind Singh IndraPrastha University, Delhi-110078, India. Email: Jloura.dgca@gmail.com

[3]Ankit Kesharwani&Shailendra Singh Bisht, The Impact of Trust and Perceived Risk on Internet Banking Adoption in India, 30 International Journal of Bank Marketing (2012).

developments in the aviation industry in India, it has undergone immense shifts. The Indian aviation sector is currently deemed private, whether it is operated by the Government, with full-service airways and moderate carriers. Commercial airlines make up over 75% of the local aviation market[4]. Before, they treated many as exorbitant, controlled and benefited methods of transport. In a country's economic growth, aviation has been the maximum necessity fragment. It assumes that he or she would be valuable in moving people or devices from nearby to later national or foreign, particularly as the separation is long overdue.

There is a rising degree of connectivity and digitalization in the air transport chain. In the aviation industry, technical developments allow huge chances to enhance not only customer care, protection, flight quality, operations but also the experience of passengers on the ground as well as in the air. The industry has become more open and vulnerable to cyber-attacks on harmful viruses aimed at the aviation sector through technical advancements and connections. Detection and avoidance is the best-looking approach because after each attack these risks get steeper and steeper. The need for technological developments to prevent IT infrastructure and networks in the aviation sector from cyber-attacks is the main factor for this business. Moreover, the need to secure the infrastructure is crucial as the spacecraft industry progresses towards autonomy and invests billions into aviation technology growth[5] . For its ground and flight activities, the aviation sector relies heavily on IT infrastructure. The safety of these airline networks has a significant effect on the industry's safety and performance and indirect effects on operation, prestige and financial wellbeing.

II. INTERNATIONAL REGULATIONS

International Civil Aviation Organization, (ICAO) is the specialized agency of United Nations, through which the techniques and principles of air navigation, across the globe, are codified. ICAO is responsible for fostering the planning and the development aspects of the global air transport, in a safe, orderly and expeditious manner. ICAO was given the key duties of technical standard setting, accompanied by the overall generic supervisory functions[6]. The strategic objectives of ICAO included

- Security and facilitation
- Environmental protection
- Safety
- Air navigation capacity and efficiency
- Economic development of air transport[7] .

ICAO has established 19 Annexes to the Convention on the Civil Aviation Organization.

---

[4]Alok Kumar Singh, Modelling Enablers of TQM to Improve Airline Performance, 30 International Journal of Productivity and Performance Management (2013).

[5]Bhavya Malhotra, Foreign Direct Investment: Impact on Indian Economy, 4 Global Journal of Business Management and Information Technology (2014).

[6]L Weber, Encyclopaedia of Public International Law, Vol. I 571 (1992).

[7]ICAO,Annual Report of the ICAO Council: 2014 (2014) (Mar. 05, 2021 08:20pm) https://www.icao.int/annual-report-2014/Pages/default.aspx

ICAO has the responsibility of regulating the Aviation security worldwide through the Annex 17 and its various resolutions.

The security feature of air law is primarily concerned with the following:

- The Tokyo Convention of 1963's Offences and some other acts taken place on board aircraft;
- The Hague Convention of 1970's subdual of illegal seizure of aircraft; and
- The Montréal Convention of 1971's subdual of illegal acts against the safety of civil aviation.

At present, Annex 17 covered under Chapter 4 deals with the cyber threats which inter-alia states that:

"....Each Contracting State must develop measures in order to protect information and communication technology systems used for civil aviation purposes from interference that may jeopardize the safety of civil aviation."

In the 2019 ICAO Cyber-security Aviation Plan, capability development and the culture of cyber-security were recognised and discussed, as core components of a successful cyber resilience programme [8].

III. NATIONAL REGULATIONS

A. INFORMATION TECHNOLOGY ACT, 2000

In 1996, to encourage global regulatory uniformity, the UN International Trade Commission introduced the e-commerce model rule. This model legislation has been approved by the UN General Assembly as the basis of numerous cyber rules. India quickly became the 12th nation in the world to legitimize cyber laws[9]. Post the first draft, established in 1998 by the Ministry of Commerce under the E-Commerce Act, adopted in May 2000 by revised Bill on information technology[10]. Finally, with the implementation of the IT Act in October 2000, things were under regulation. This Act carefully traced any trifle online, cyber and worldwide Network operation or purchase[11]. The small behaviours and the global cyberspace response levied significant legal consequences and penalties. The act soon altered the Indian Penal Code (IPC) 1860 (45 of 1860), the Bankers' Books Evidence Act 1891 (18 of 1891), the Indian Evidence Act (IEA), 1872 (1 of 1872) and the Reserve Bank of India (RBI) Act 1934[12] . These reforms intended to provide legal recognition for transactions carried out by Electronic data interchange.

The penalty for cybercrime is protected by Section 66F[13]. This portion will be considered

---

[8]John Macilree,&David Timothy Duval, Aero politics in a Post-Covid-19 World, 88 Journal of Air Transport Management (2020).

[9]Vinit Kumar Gunjan et al., A Survey of Cyber Crime in India, 88 15th International Conference on Advanced Computing Technologies (ICACT) (2013).

[10] Information Technology Act (2000).

[11]Jamal Raiyn, A Survey of Cyber Attack Detection Strategies, 8 International Journal of Security and Its Applications. (2014).

[12]Stephen J Lukasik et al., Protecting Critical Infrastructures Against Cyber-Attack (2020).

[13]Information Technology Act § 66 (2000).

to have detrimental effects on vital facilities in circumstances when either of three forms of defined operations resulting in injury or death to any individual caused or significant harm to supplies, utilities, property or disturbances that are important to a community existence is carried out[14]. These infrastructures are defined by section 70 of this Act as secure networks[15]. In this clause, the person who violates the requirements of the respective sections shall be punished up to 10 years and fined. Section 70B[16] creates an "Indian Computer Emergency Response Team" for support in electronic protection accidents and other cyber-safety-related emergencies[17] .

The IT Act requires any device to be designated as a security mechanism by the proper government, with direct or indirect consequences for the CII facility, as well as CII. When informed as a "protected system," the CII shall be granted protections against any improper disorder or access using tighter regulations. In some cases, this feature of CII considered being "protected systems." These involve the UIDAI Servers, the Terra Protected Network, and the Long Range Detection and Tracking Device. The banking and financial processes have also been monitored. However, the broad importance of the protected structure has contributed to the goal to define regions that ought to be protected. This includes the case of governmental governments such as the government of Chhattisgarh which interpret these systems openly to include any kind of network connections and computer systems.

B. THE NATIONAL CYBER SECURITY POLICY, 2013

The cited policy expressed cyberspace as a shared resource for disparate players that are not readily distinguishable from each other, as was cyber-security. This policy determines the different ways that cyber protection can be successfully managed. These approaches include threats detection, intelligence exchange between stakeholders, survey and response planning. The key aim of this policy was to demonstrate how crucial it is to secure personal data from cybercrime and the vital infrastructure economic and socially[18]. While this strategy acknowledged the numerous facets of cyber-security, it had not differentiated between disparate approaches to national cyber-security and the way the government plans to address these concerns. This involves failing to explain how cyber threats or cyber-terrorism need to be handled while coping with the sensitive infrastructure of data loss cyber threat. Such deficiencies involve a shortage of material interventions or goals to accomplish cyber-security

[14]Debarati Halder, A Retrospective Analysis of S.66a: Could S.66a of the Information Technology Act Be Reconsidered for Regulating 'Bad Talk' in the Internet?, 3 Indian Student Law Review (ISLR). (2015).

[15]Information Technology Act § 70 (2000).

[16]Information Technology Act § 70B (2000).

[17]Dr. Rajinder Kaur& Dr. Rashmi Aggarwal, The Information Technology Act, 2000-Demystified With Reference to Cybercrimes, 17 Paradigm (2013).

[18]Sanjiv Tomar, National Cyber Security Policy 2013: An Assessment, Idsa.In (Mar. 06, 2021, 05:25am)https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813#:~:text=With%20an%20aim%20to%20monitor,citizens%2C%20businesses%20and%20the%20government.

C. XII FIVE YEAR PLAN REPORT ON CYBER SECURITY (2017- 2022)

To conform to unclear laws, the "XII Five Year Plan Report on Cyber Security" is another step taken in India. This strategy applies from 2017 to 2022 with the emphasis on seeking solutions to ensure cyber-security in a comprehensive way over the expected span. Certain concrete measures have been established, which can be viewed as the aim results for cyber defence. The only problem is that only a couple of them are working[19].

In cyber defence policies, and even in the five-year strategy, cyberspace offenders are listed as being a concern. Cyber-warfare, identity stealing, hacking and similar offences are other crimes that can be investigated by law enforcement authorities in compliance with several provisions of the IT Act (2000) of the IPC. In addition to being no precise line of policy for Internet-based crimes, there is also a very small distinction between the cyber-dependent and cyber-enabled crimes[20]. There is still a shortage of legislation specific to regulatory authority on data privacy. The reality is that the safety of specific personal records, typically owned by private individuals, as the main aspect of cyber-security, is barely any prominence in legislation. Market instances and privacy security vis-à-vis web platforms are mostly dominated by privacy laws, particularly those related to statutory solutions.

The primary mechanism for data security, as required by the IT Act in Section 43A "body corporate," remains to be the provision of fair practices[21]. They are read regarding the Requirements for Appropriate Protection Procedures, which state the need to conform to sound safety standards. These requirements are contained in the numerous manuals, including the "ISO 27001 Information Security Management Norm" with the help of the Government. The national cyber-security, including strategy for the private sector, community and government policies, has taken increasing importance for the country. These are once again reliant on the internet and hence the need to maintain the same. Furthermore, the nation'scyber protection system has shown a strong need to protect economically and socially important sectors (including insurance, banking and energy), and the nation's cyber-security is seen as a key component of the nation's defence goals and foreign policy[22]. And as a variety of variables presenting "cyber-security threat" (including foreign governments, terrorists, incidents or natural disasters) are recognised in the cyber-security strategy, this policy remains primarily directed towards the coordinated cyber challenges (including the ones by terrorist groups or foreign states). They can pose public safety risks, which is why cyber-security is not seen by a multifaceted strategy, with an important emphasis on achieving state and nation-based targets using this policy. In comparison, the Indian strategy emphasizes developing cyber-security techniques rather than relying on cyber offence capabilities.

---

[19] Ellyne Phneah, India Govt. Unveils Five-Year Plan To Revamp Cyber-security |Zdnet, (Mar.6,2021,06:14am)https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813#:~:text=With%20an%20aim%20to%20monitor,citizens%2C%20businesses%20and%20the%20government.

[20] Chinese Academy of Cyberspace Studies, World Internet Development Report 2017 (2018).

[21] Information Technology Act § 43A (2000).

[22] Pradeep Kumar Singh et al., Proceedings Of First International Conference On Computing, Communications, And Cyber-Security (IC4S 2019) (2020).

IV. CYBER SECURITY IN AIRPORTS

A. REVENUE GENERATING STREAM

One of the key trends in airport management stems from the fact that the passenger's contact point is a major market share. This is because the number of passengers travelling by air is rapidly increasing, particularly in a nation like India[23] . This is the reason why airports do continue to bring improvements in infrastructure intelligence so that they can ensure that the passenger's travelling experience is improved. When there is a real-time exchange of information to the likes of the flight schedule, the airport-wide process integration, and collaborations, the airports can improve their passenger services, advanced security capabilities and operational efficiencies[24] .

The 2018 SITA Air Transport IT Trends Insights report showed that the priority on cyber-security has been given particularly to the airlines and airports[25] . The statistics revealed that out of the studies airports, 94% were making a plan to invest in programs related to cyber-security by end of 2021[26]. Particularly in the context of the Asia-Pacific region, there is an increased demand for measures of cyber-security measures to be adopted in the aviation industry. The Vision 2040 of Indian Government provided that the nation needed around 200 commercial airports. This required an approximate investment of around USD 50 billion, to allow for the 1.1 billion passengers to be handled. Similar provisions were seen in the emphasis made in President's Budget of 2019 of the USA, where USD 15 billion was set aside for cyber-security measures for Airports. To secure the growing aviation ecosystem, the civil aviation authorities across the globe are focusing on ensuring and improving the security and safety standards of this face-paced industry. One of the reasons stems from the malicious malware attacks that target the aviation sector. One of such instances was noted in December 2017 at Perth Airport, where a major chunk of security data, that was sensitive, was stolen.

B. TECHNOLOGY

With the growth of technology, particularly in the context of the innovations being brought into the digital world, the world of airports is also changing. From the erstwhile days of airports, where reliance on technology was for necessities, to the present modern world of airports, where everything has been touched with technology, there has been a noted revamp in the "persona" of airports. The threats on airports, with this advent of technology, have increased manifolds. This is why the focus on cyber-security has seen a growth and new trends in this context keep on emerging with every passing year. There is a dire need for the securitization of data which has led to the adoption of strategies that demand a high level of resourcefulness in the context of sharing data[27] . This is the reason

---

[23]Vincent P Galotti, The Future Air Navigation System (FANS) (2019).

[24]Galileo Tamasi& Micaela Demichela, Risk Assessment Techniques for Civil Aviation Security, 96 Reliability Engineering & System Safety (2011).

[25]Nuriye Gures et al., Risk Assessment Techniques for Civil Aviation Security, 71 Assessing The Self-Service Technology Usage Of Y-Generation In Airline Services (2018).

[26]CISO MAG | Cyber Security Magazine, Aviation Cyber Security Market To Grow 11% During 2019 - 2024, (Mar.07, 2021, 09:00pm) https://cisomag.eccouncil.org/aviation-cyber-security-market.

[27]Paul Wilkinson& Brian Michael Jenkins, Aviation Terrorism And Security (2013).

why they need for system integration and connectivity it is increasing in the aviation industry. The constant increase in cyber-attack threats is one of the reasons for doing so.

Different airports are adopting different modes to deal with the difficulties of interoperability. Munich Airport, for instance, relies on modelling tools and data analytics for big data. This involves the use of artificial intelligence tools. The aviation industry has seen an improvement in aviation process and an evolving market, be it in context of the passenger experience improvements, advancement in air traffic management, or the enhanced efficiency of processes being adopted in airports[28]. Without such enhancements, the airports cannot be secured and controlled properly, which acts as a golden opportunity for cyber-attacks to be successful. The magnitude of these threats is catastrophic as these can result in major accidents and shutting down airports. The data and systems adopted in airports is a target for hackers, where they can also take a chunk of money from the airports, just to give the control system of airports back to the right authority[29] .

One of the recent trends noted in airports' cyber-security is Block Chain. This is a technology that is being deemed as a safe and reliable mode of exchanging the key information that is held in the digital channels. The main reason for relying on this technology stems from the need of securing the financial value assets' exchange. Though, the use of the principles and application of Block Chain technology, in realms of aviation information technology is still being researched[30]. Various prototypes are not only in a development phase but also some which have landed the testing phase. This technology does offer some promising solutions. But as is the case with every technology, this technology too comes with its own set of challenges, specifically in the context of its cost of operation and its governance. These measures are still being discussed and sorted out.

The basic concept that eases the airport system with the use of Block Chain is that it supports and challenges the barriers that are present between the individual procedures as the data is locked in a shared Block Chain[31]. This is better from erstwhile systems of the need of accessing/ consulting with the central authorities to get the personal data. Essentially, Block Chain makes the entire system efficient by making it simpler. An example of this can be cited in Digital identity concept. In this matter, the identity of a person can be stored in a network, which could give away the need for showing the travel documents and passport during the journey, at the airports[32] . There is also the ease of a new booking platform being implemented, as is being done by companies like

[28]Sorin Eugen Zaharia& Casandra Venera Pietreanu, Challenges in Airport Digital Transformation, 35 Assessing The Self-Service Technology Usage Of Y-Generation In Airline Services (2018).

[29]Mark G Stewart& John Mueller, Terrorism Risks and Cost-Benefit Analysis of Aviation Security, 33 Risk Analysis (2012).

[30]Assunta Di Vaio& Luisa Varriale, Block Chain Technology in Supply Chain Management for Sustainable Performance: Evidence From the Airport Industry, 52 International Journal of Information Management. (2020).

[31]R. I. R Abeyratne, Aviation In The Digital Age (2020).

[32]Qiang Cui& Ye Li, The Change Trend and Influencing Factors of Civil Aviation Safety Efficiency: The Case of Chinese Airline Companies, 75 Safety Science (2015).

Travel Block or Winding Tree. There is also a possibility of different rewards systems being unified.

A study conducted by British Airways, Miami, Heathrow and Geneva Airports and SITA known as Flight-chain highlighted how the Block Chain technology is used to solve different issues as it creates a single source of truth. This is because the flight information is updated as soon as everyone agrees to it. The attacks done in recent times at airports like Gatwick Airport have highlighted the need for thinking about airport operations and drones. There is a development of Block Chain-based app being done by Brussels Airport for replacing the handover documents from that of the handlers to that of the forwarders[33] .

Another noted trend that is meant to ease and help in the rise of interoperability involves SWIM, which stands for System-Wide Information Management. This is a technology program that is brought forth by ICAO and is being developed in single European Sky ATM Research (SESAR). The goal here is to set out common standards that can be adopted for exchanging the data, in a safe and secure mode. This is because the airports do provide a scalable and flexible architecture that can allow for proper and consistent information being exchanged, thereby improving both the operations and planning at airports. The other noted technological advancements that have been adopted by the airports in the context of cyber-security involve use of automation, Internet of Things (IoT), Artificial Intelligence (AI) and cloud computing[34] .

With the 2020 pandemic, the growth of AI has seen an upward swing. This is because of the need to further digitizing and taking out the human element, to contain the spread of viruses like COVID having resulted in reliance being placed on AI[35] . Even though AI has been here for many years, it is noted that there has been slow progress of it in airports. The things like Chabot and robots have seen their way in airports, but the lack of enhanced systems of these AIs have resulted in a very restricted adoption in reality. The Seattle-Tacoma International Airport and London Heathrow Airport have seen a trialling AI tech whereby the turnaround process video footage is being captured and compared based on the already planned schedules. In Germany, the Fraport is making use of machine learning for predicting the flight touchdown, based on flight tracking timestamps that are available in hundreds of thousands[36] . The best part is the possibility of improving the genius of AI. This is in sense of the improvements in passenger and aircraft process by making better predictions regarding the various experiences available at the entire airport.

C. CHALLENGES POSED BY CURRENT TRENDS

All the aforementioned advancements come with high costs. And the key problem here is that the value of these technologies is not assured. This is because the cyber threat

[33] R. I. R Abeyratne, Aviation Trends In The New Millennium (2017).

[34] Achim I Czerny et al., Post Pandemic Aviation Market Recovery: Experience and Lessons From China, 90 Safety Science (2021).

[35] Kaitano Dube et al., COVID-19 Pandemic and Prospects for Recovery of the Global Aviation Industry, 92 Journal of Air Transport Management (2021).

[36] Dagi Geister&Robert Geister, Integrating Unmanned Aircraft Efficiently Into Hub Airport Approach Procedures, 60 Navigation (2013).

landscape is involving technology and is also relying on the same technology to counter the predecessor. A global estimate put the slower pace of technological innovation in cyber-security amounting to a threat of lost USD 3 trillion for 2020. Some of the reasons being, the complex regulatory requirements, dangerous insider threats, skilled security personnel and incessantly evolution of cyber-attacks. The pandemic acted as another major security challenge for the airports. This is because the complexity of data breach grew in 2020, where the breaches increased by 273% in just the very first quarter when compared to the same value of 2019. A single hacker was able to steal 34 million user records in 2020 from 17 companies[37] .

V. CYBER BREACH IN INDIA

A. SPICE JET AIRLINE CASE

The confidential details of over a million travellers have been leaked through a data leak on the Indian Spice Jet airline. A technology researcher who documented an intrusion to Tech Crunch obtained entry to the operating system of the airline.The researcher fetched an unencrypted archive backup file that included private details from more than 1.2 million passengers travelling over Spice Jet, utilizing a brute force attack. The password securing the data was easy to conjecture, according to the ethical hacker[38] .

The violation details contained the names of travellers, contact numbers, email instructions, and birth dates. Several government officials were among the passengers whose details were revealed. According to the researcher, it was straightforward for someone who knew where to go to the database file to make the budget airline insecure. After the illegal access to passenger data of Spice Jet was effectively acquired, the prosecutor approached the airline to notify them of a violation[39] . The researchers said they made no positive reaction to Spice Jet's attempts to meet the airline.

B. INDIGO AIRLINE CASE

India's largest fleet-sized airline, Indigo has reported that hackers have possibly infected some of its internal records. The carrier announced during the filing in BSE that several of its servers were compromised in December. It is claimed that, while "some segments of data servers" have been infringed, the networks have been restored in a very short period with minimal effects. "There is a risk that the hackers will publish any internal documents to public websites and forums. We understand the gravity of the problem and continue to collaborate with all the necessary experts and law enforcement to maintain a thorough inquiry into the event [40]."

---

[37]Marco Scholz&Fethi Abdelmoula,, Active Noise Abatement Using the New Developed Pilot Assistance System LNAS, Institute of Noise Control Engineering (2017).

[38]Navid Kagalwalla& Prathamesh P. Churi,, Cyber-Security in Aviation: An Intrinsic Review, 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA) (2019).

[39]Clarence C Rodrigues et al., Commercial Aviation Safety (2017).

[40]Cirium, Indigo Investigates Data Breach Involving Internal Documents, Flight Global (Mar. 08,2021, 10:08am) https://www.flightglobal.com/airlines/indigo-investigates-data-breach-involving-internal-documents/141803.article.

C. IGI AIRPORT (DIAL) CASE

The passengers of IGI (Indira Gandhi International) airport were left stranded on 29th July 2011, and the flights on Terminal 3 of Delhi were delayed. Instead of automated check-ins the same had to be done manually for the flights. DIAL (Delhi International Airport Limited) claimed that this was merely a back end server glitch. This incident covered 50 flights being impacted owing to failure of CUPPS(Common Use Passenger Processing Systems), as the domain was not working for around twelve hours. Further, it was restored only when ARINC (Aeronautical Radio INC.) and Wipro intervened. Even though no flights had to be cancelled, several of them were delayed by around half an hour.

Upon the investigation of CBI (Central Bureau of Investigation) of India, this simple technical failure was a virus attack on the system. A case was registered under the Indian IT Act where the investigations revealed that a malicious code was used, and that too from an unknown remote location, resulting in the failure of CUPPS. As per CBI, this was triggered through some scripts on system, which pointed towards the involvement of experts holding detailed and expertise knowledge regarding these systems, along with holding the intent of crippling these systems. As this was deemed as a type of cyber-attack, CBI looked for the responsible individuals, resulting in case being filed against unidentified people. CBI also concluded that there were major security lapses[41].

There were reports of other such incidents as well. As per one of such reports, a server covering 148 domains of airports of India (including Trivandrum and Cochin), were hacked by Pakistani cyber criminals. These individuals were identified as being Pak Cyber Attackers, named Kashmiri Cheetah[42].

VI. CONCLUSION

While there are several views on how to develop a common view of the aviation cyber-security challenge, there is potential for and a move forward. Adversaries have a large attack surface and potential, with growing numeration and accessibility. A further weakening of physical controls which shielded the aviation industry so long is the increasing complexities of systems, procedures, and supply chains, combined with an increase in wireless connectivity. In addition to highly competent threat entities, the aviation industry faces an essential challenge, spanning from terrorists to nations. Where necessary the industry wants to pursue rapid gains, but still understand that it is still an evolving challenge to protect the aviation industry from cyber adversaries.

India saw the confidence in digital forms much later than its foreign partners. That is why it has taken cyber-security steps well behind nations such as the USA and the other European nations. Yet again, that is why the electronic protection initiatives for the civil

[41]Manan Kakkar, CBI believes cyber-attack led to IGI airport's technical problems in June, (Mar. 08, 2021, 11:28pm), https://www.zdnet.com/article/cbi-believes-cyber-attack-led-to-igi-airports-technical-problems-in-june.

[42]Surbhi Gloria Singh, Major cyber-attacks across the globe, (Mar. 09, 2021, 11:55 pm), https://www.business-standard.com/article/technology/2016-a-year-for-hackers-spies-know-major-cyber-attacks-across-the-globe-116122800341_1.html.

aviation industry have been postponed. BCAS, which looks at aviation security concerns, is the main body operating in this region. Steps are taken, such as control rooms and staff preparation. The Information Technology Act, 2000 is the key law protecting the Indian cyberspace. The Indian cyberspace has been effectively secured by initiatives like the National data protection strategy, the "XII Five Years Plan Report on cyber-security" and so on. The fact that they are not constructive is a crucial negative feature of Indian Internet protection legislation. These activities are to be taken after international cyberspace comparison. Even if this is not a negative problem, it demonstrates that dependence on others is still important to take the measures needed to defend cyber-areas in civil aviation. There are also just a couple of initiatives operating in the area of aviation cyber protection in terms of regulatory instruments and bodies.