International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

Role of Information Technology in Civil Aviation: A Focus on Cyber Crimes and Emerging Legal Issues

Dr. Shaik Nazim Ahmed Shafi[♣]

[♣]Assistant Professor of Law, NALSAR University of Law, Hyderabad

Introduction

The initiation of the concept of liberalization, privatization and globalization with highly advanced technology blended with information technology has completely transformed the economic behaviour of the world. Civil aviation is one of the most widespread and extensively interconnected international infrastructures in the world connecting everyone, every time and in every place. 'Airports' and 'Airlines' are the economic engines for the growth and development of a nation.[1] Civil aviation is a glamorous industry but sensitive and yet its abuse has become a threat to the general security of passengers, crew members and aviation industry as a whole due to the misuse of information technology. Today every airport, airline and the air traffic control systems are based on intelligent transport system i.e. the information and communication technology (ICT). Aviation has become the backbone of our global economy bringing people to business, tourists to vacation destinations and products to markets.

"Aviation" is the business of freedom. In 2016, 3.8 billion passengers safely took to the air and some 54.9 million tonnes of goods were delivered as air cargo.[2] Focusing the "financial performance"aviation's vital role in the world has not always resulted in appropriate rewards to airline investors. In recent years, however, airline efforts to restructure and reengineer their businesses have resulted in a historic strengthening of the bottom line. The industry earned a return on invested capital of 9.9% in 2016[3], which exceeded its cost of capital (estimated at 6.6%). Regarding the "safety", flying safely is the number one priority and the industry competes fiercely for every passenger, but there is no competition when it comes to ensuring safety.[4]Pointing out at the "aviation security", the aviation industry continues to be an iconic target for terrorist and other security-related attacks.

The purpose of this paperis to divulge how information technology is the key element in the economic development of aviation industry as a whole and airports, airlines and air traffic control system in particular. This paper also tries to focus the impact of information technology paving way for cyber-crimes etc. and existence of any legal mechanism to curb the said issues focusing the International Conventions pertaining to civil aviation and cyber-security.

Role of Information Technology in Aviation Industry

Air travel has always been closely connected with the information and communication technologies (ICT), benefiting from the technological developments and, in the same time contributing to its evolution. The modern consumer is more familiar with IT technologies; he has access to information which made him more sophisticated and demanding, requiring specialized and interactive services. The evolution of ICT shaped and

[♣]Assistant Professor of Law, NALSAR University of Law, Hyderabad

1. *Airports Privatisation in India: Law and Policy Issues* (1st ed., pp.102). (2013). Hyderabad, Andhra Pradesh: Asia Law House.
2. IATA Annual Review-2017
3. IATA Report-2016
4. IATA Report 2016: One major accident for every 2.56 million flights using jet aircraft in 2016.

re-engineered the air travel industry globally.[5] The air travel linked with tourism industry is highly fragmented and diverse, linking a "worldwide supplier community"[6] with passengers/consumers being distributed globally. The evolution of ICTs demonstrated that centralizing data is a key element in the development of air travel and tourism as well as transforming distribution into an electronic marketplace.[7]

The pioneers of the technical developments in the air travel and tourism industry were the Computer Reservation Systems (CRS) in the 1970s and the Global Distribution Systems (GDS) in the 1980s, among the first multi-organizational and global information systems[8] followed by the Internet in 1990s a first step associated to the development of the "world wide web"[9] under the 20th century. However, the 21st century has witnessed an advanced technological development which has transformed the aviation industry. Digital technologies have been the driving factor for improving airlines' operational efficiency. Custom software application development has become a major contributor to a company's competitive advantage and garners exponential growth in business. It helps the industry to leverage its technology and services by extracting full potential. It also facilitates the implementation and development of global standards and delivers value to the airline business firms.

The advent of technology and social media is increasing the customers' expectation to build and increase their relationship with the organization. Understanding customers' preferences, IT innovation and modernization help the airlines re-engineer their business processes by addressing the industry challenges and opportunities and transform its practices to a customer-centric approach. This conventional approach increases the connectivity and enhances the customers' satisfaction and innovative software applications provide real-time value to the customers.

Market conditions and industry developments affect the growth of any business. The increase in traffic and competitive pressure has been adversely impacting the financial sustainability of the airline industry. The current global market conditions and industry developments coupled with evolving technological trends and customer preferences are introducing more challenges than ever before. IT automation has removed barriers and changed the landscape of aviation industry. It helps the industry in cutting costs, improving relationships with the customers and clients, and improving the financial performance in a sustainable way.

The aviation operations since decades are based on IT industry. The aviation industry widely uses a variety of applications through the digitalization of different procedures. A catalogue of solutions can be found helping airlines manage a variety of processes, such as electronic documentation, aircraft performance and flight planning optimization, crew management or fuel efficiency. Other new services have recently become available, such as solutions for live flight tracking.

Data analytics is not an exception and in the last few years a number of companies have started to incorporate functionalities based on data mining and machine learning. A second generation of data analytics applications will surely disrupt traditional operational procedures by fusing a variety of data sources, including not just airline or weather data but also airspace management data. Applications will be able to fuse and analyze a variety of datasets and leverage historical behavior of the system to predict and recommend operational solutions to airlines, airports and air navigation service providers.[10]

Taking the IT into consideration, presently, several companies are promising increased efficiencies in different contexts like the Navblue, an Airbus company, offering the N-software, able to produce best-in-class

5. Buhalis Dimitrios, Strategic use of information technologies in the tourism industry, p.3
6. Werthner H, Klein S, ICT and the changing landscape of global tourism distribution, Electronic Markets, Volume 9, Issue 4, 1999
7. Buhalis Dimitrios, Strategic use of information technologies in the tourism industry, p.6
8. Abel Usoro, ICT (Information and Communications Technologies) and Tourism: An Initial Exploratory Study of Developing Economies as Suppliers of Hospitality and Destination, p. 1
9. Mistilis N, Buhalis D, Challenges and potential of the Semantic Web for tourism, eRTR, vol 10, 2012, p. 51
10. Perez, D. (2017, March 16). How the Information Technology is disrupting aviation data analytic? Retrieved from http:// http://datascience.aero/information-technology-industry/

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 5, Issue 1
January 2018

aero data targeting airspace re-design; Sky-breath, offered by Open Airlines, promises to exceed 2% on fuel savings thanks to big data analysis; Honeywell software helps airline flight operations managers to quickly understand fuel consumption trends, identify savings opportunities, monitor progress of savings initiatives and demonstrate results; PACE offers a more effective fuel management through improvement of daily operations, strategic planning and operational efficiency; and UTC offers enabling improvements in operational efficiency by integrating flight planning, avionics data, flight performance tracking and weather data with real-time updates and notifications.

Focusing on terms of aviation safety, Flight Data Services offers a full analysis service to aircraft operators to gain valuable safety insights through detailed reporting, statistics and visualization directly to safety departments. In addition, Flight Scanner, offered by Safety Line, offers to automatically identify the factors associated with hazardous situations based on all flight data. Last but not least, Innaxis coordinates the Safe-Clouds.eu research project which develops new data analytic techniques for a variety of airline and air traffic control operational contexts.

As the technology sector moves forward faster than other industries can keep up, the future seems at once both exciting and worrying i.e. issues such as cyber security becomes more and more challenging at a faster and faster rate. The year 2017 has revolutionized various technologies in the aviation and airport industry like that of Blockchain technology, Game of Drones, Augmented Reality, Chatbots, Airline New Distribution Capability and Indoor Positioning Systems (Beacons Technology).[11]

a) **Information Technology in Airports:** The establishment of the Airport Council International[12] (ACI) World Airport Information Technology Standing Committee (AITSC) has had paved way for the development of industrial policy guidelines and positions on issues affecting Information Technology (IT), Airport Automation, Telecommunications infrastructure and related passenger and cargo services at airports, in order to support operational and business processes in and around airports. The AITSC monitors developments in procedures, technologies and policy related to or that will impact Airport IT as well as discusses and examines functions of an airport that could benefit from automation. Also, the Standing Committee actively works to convey information to the airport community on all airport IT related issues, from practical and physical applications to new policy and guidelines. However, the AITSC deals with current issues like the common use self-service devices for passengers, electronic kiosks and other means of information distribution; machine readable travel documents (MRTD); passenger and baggage security (in the context of airport automation); information exchange and interconnection of various non ACI entities.

Airport Council International (ACI) believes that it is important to have a strong position on biometrics with the increase need in securing personal identification. 'The Application of Biometrics at Airports' provides general recommendations on the development and implementation of biometrically enabled programmes for border control, passenger facilitation and staff access control.[13]

b) **Information Technology in Airlines:** In a hyper-competitive environment, with tight margins and increasing regulatory and environmental pressures, airlines have for many years looked to technology to deliver greater operational efficiency. Now digital has ushered in opportunities for creating and delivering differentiated customer experiences that can build loyalty. And in a market place where it's harder than ever to stand out, that's absolutely critical.

Airlines have reached a defining moment.[14] The industry knows that digital will transform their industry.[15]The five key trends that together made Technology Vision and drawing out the most

11. https://www.internationalairportreview.com/article/26374/technology-revolutionise-aviation-2017/
12. Retrieved from http://www.aci.aero/About-ACI/Overview/Standing-Committees/Airports-Information-Technology
13. Annex 17: Security-Safeguarding International Civil Aviation Against Acts of Unlawful Interference, International Civil Aviation Organization (ICAO).
14. For example: For example, Virgin America is a front-runner that has learned to think like the disruptive tech businesses that surround it in Silicon Valley. Virgin has experimented with everything from in-flight social

relevant implications and manifestations for the global airline industry are; (i) Adoption of automation; (ii) Liquid workforce – flexibility for today's digital demands i.e. sophisticated augmented reality (AR) technologies;[16] (iii) Platform economy – an innovation from the outside, in i.e. airlines will create interface on their proprietary platforms via Application Programming Interface (APIs), extending connections to other participants in the travel economy; (iv) Predictable disruption – digital ecosystems drive the next wave of change i.e. they need to develop greater predictive analytics capabilities that can harness developments outside their industry and map the potential impacts; (v) Digital trust – strengthening customer relationships through ethics and security. But, while this means airlines have little trouble in gathering customer data, they are also somewhat restricted in how they can use it beyond its immediate purpose.

Hence, trends in technology impact all industries, and travel and aviation is no exception. To stay competitive, airlines must use the newest technology to offer customers a better travel experience.[17] Some of the emerging technologies in the airline industry are; connectivity; passenger empowerment; biometrics, sensors and tracking technology, virtual reality, improving security, and cloud solutions.

c) **Information Technology in Air Traffic Control System:** The present air traffic control (ATC) systemhas evolved over several decades from the onethat was first put in place in the 1930's. The operationalcharacteristics and organization of theoriginalsystem were determined largely by thetechnologiesthen available—radio for navigation and air/ground communication, and telephoneand teletype networks for distribution ofinformationamong ATC ground facilities. Newtechnologies—such as Surveillance radar,Air Traffic Control Radar Beacon System(ATCRBS) transponders, microwave relays, andelectronic data processing—were added as demandincreased and the State-of-the-Art progressed after World War II, but they did notchange the essential characteristics of the earliergeneration of air traffic control—a ground based,labour-intensive, and increasingly centralizedsystem.[18]

Advanced data-processing and communication technologies have been introduced to meet the growing demand for ATC services[19] and to provide the controller with the information needed to make the decisions required for the safe and efficient movement of aircraft. However, these technologies were applied largely to improve the acquisition, integration, and display of formation, or to speed its dissemination among ATC facilities. Recently, the automated transmission of certain types of information to pilots has also been introduced, e.g., weather and terminal area briefings. However, the making of ATC decisions and transmission of ATC messages have remained essentially a human function.

The requirements for the ATC system will be affected as and when the air transportation network grows and evolves in response to economic conditions, market forces and changing government regulations. In addition, new technological developments will make possible new functions and modes of operation that would have been impossible with older equipment and resources. The character of the ATC is depended upon the latest technology being used by the air traffic controllers. At times it becomes a budgetary constraint on governments how much to be paid to the service providers.

---

networks to rethinking how to buy tickets. It went as far as collaborating with its frequent flyers to secure two gates at Dallas Love Field. 30000 people signed a Change.org petition to allocate these gates to the airline. In return, the airline offered pre-IPO stock optionsto frequent flyers. The collaboration may have been virtual, but the rewards have been very real: revenues of almost US$ 1.5 billion in 2014 and a US$ 306 million initial public offering (IPO)

15. Turbulence ahead: Plotting a course through digital disruption-Technology Vision for Airlines 2016.
16. Ibid
17. Philip Te Hau, http://www.digitalistmag.com/customer-experience/2017/08/14/emerging-technology-in-airline-industry-05226935
18. Chapter 5. Technology and the Future Evolution of the ATC System. (n.d.) In *Air Traffic Control* (pp.67- 77). Retrieved December 14, 2017, from http://www.princeton.edu/~ota/disk3/1982/8202/820207.PDF.
19. These technologies have also found use in the cockpit where RNAV and other systems have provided capabilities that have indirectly affected the ATC system.

In order to accomplish the goals of safety, efficiency, and cost-effective operation, the present ATC system offers various services to the aviation community like the separation assurance[20]; navigation aids[21]; weather and flight information[22]; traffic management[23]; and landing.[24]These services together comprise an integratedprogram, no part of which can be fully effectivewithout the others. Flight plans must take into account weather and traffic, for instance, traffic must be routed to destinations so that it arrives on time and can be handled at the airportwith a minimum of delay.

Similarly, clearanceshave to be modified so that traffic can be routedaround severe weather or away from bottle-necks that develop in the system. In a practicalsense, the aircrew and ground controllers cooperateas a team using various human and electronic resources to maintain safety and to movetraffic expeditiously. While the ultimate responsibilityfor safety of flight rests with the pilot, heremainsdependent in many ways on data or decisions from the ground. However, the major equipment components that support these ATC facilities are surveillance radar, airborne transponders, navigation aids, computers and communication links.

Cyber Crimes and Aviation Security: The Emerging Legal Issues

Aviation security is mainly classified into two; (i) Airport Security which includes customers, airport property, air traffic controller, cargo and airport operating systems; (ii) Airline Security which includes; passenger, crew, cargo, aircraft, flight management systems, and airline operating systems. The aviation security is important in a manner that the global economic value of aviation industryis estimated to more than 2.2 trillion dollars. However, the said industry is not free from global threats like from hackers and terrorists. The present day innovative advanced information and communication technology has misled the aviation industry a new growing type of threat from cyber space. As the industry relies more on information and communication technology (ICT), it is prone for security breach from hackers and terrorists.

The aviation sector is not immune to the cyber security risks that have been critical issues for all other industries.[25]It isn't just navigation systems that have been subject to cyber-attacks. An attack on the internet in 2006 forced the US Federal Aviation Administration (FAA) to shut downsome of its air traffic control systems in Alaska. In July 2013, an attack led to theshutdown of the passport control systems at the departure terminals at Istanbulairport, causing many flights to be delayed. Finally, an attack that possiblyinvolved malicious hacking and phishing targeted 75 airports in the USA in 2013.These are just a few examples among many more but they justify the needs toprevent such threats that could lead to dramatic consequences.

Today, the ITC has removed the gap between the people (hackers and terrorists) and the devices by which security threat in aviation sector has emerged. One of the major explanations for this new type of threat in this sector is the greater use of computer-based systems: sophisticated air navigation systems, on-board aircraft control and communication systems, airport ground systems including flight information and security screening, day-to-day management systems etc. In the same time, cyber threats have been developed

20. Tracking aircraft in flight, primarily with surveillance radars on the ground and airborne transponders, in order to ensure that adequate separation is maintained and to detect and resolve conflicts as they arise
21. Maintaining a system of defined airways and aids to navigation and establishing procedures for their use.
22. Informing users of the conditions that may be expected along the intended route so they may plan a safe and efficient flight.
23. Processing and comparing the flight plans, distributing flight plans to allow controllers to keep track of intended routes and anticipate potential conflicts, and ensuring the smooth and efficient flow of traffic in order to minimize costly congestion and delays.
24. Service operating airport control towers; instrument landing systems, and other aids that facilitate the movement of air traffic in the vicinity of airports and runways, particularly during peak periods or bad weather that might affect safety or capacity.
25. Duchamp H., Bayram, I., & Korhani, R. (2016, June 30). Cyber-Security, a new challenge for the aviation and automotive industries. Retrieved December 15, 2017, from http://blogs.harvard.edu/cybersecurity/files/2017/01/Cybersecurity-aviation-strategic-report.pdf

regardless of the industries but in relation with technologies: computer viruses, malicious attacks, etc. Like any other industry, it is possible to consider two types of cyber security breaches i.e. (i) opportunistic – here the goal is to exploit mistakes made by internal users like employees using the IT systems with the purpose of causing inconvenience and nuisance to any entity involved in the aviation ecosystem; and (ii) calculated and premeditatedi.e. it concerns any malicious attacks to disrupt operations or threaten lives. This category is critical as terrorists are fully aware of the potential of technologies and cyber-attacks.

a) **Categories of Cyber Crimes in Aviation Industry:** "Airport security"refers to the techniques and methods used in protecting passengers, staff and aircraft which use the airports from accidental/malicious harm, crime and other threats. Airport threats could be cyber-attack, sabotage, improvised explosives devices (IED), border security, traffic of unauthorized materials and other security threats. However, "airport security" can be breached through cyber-attacks in the following ways[26]:

i. GPS Spoofing and Jamming: Spoofing is an attempt to deceive a GPS receiver by broadcasting counterfeit GPS signals, structured to resemble a set of normal GPS signals, or by rebroadcasting genuine signals captured elsewhere or at a different time.[27] Jamming is applied to knock out the navigation system entirely. Jammers can disrupt civil aviation systems and emergency service communications.
ii. Air Traffic Control (ATC) Hacking: Hackers could gain access to communication between aircraft and ATC centers and send false information to mislead pilots or overwhelm controllers with fake aircraft signals.
iii. Security Threat to Airport Operating Systems: Airport infrastructure supports many different operations that are critical for the efficiency and effectiveness of the air transport system making cyber-security system implementation essential to protect and control those operations. There have been incidents when cyber criminals, hackers have found opportunity to attack airport systems.[28]
iv. Security Threat to Airport Security System: Several potential targets for cyber-attacks within the realm of internal airport operations like; access control and perimeter intrusion systems, radar systems, ground radar, network-enabled baggage systems, supervisory control and data acquisition (SCADA). Airports typically rely on SCADA-type industrial control systems for utilities, baggage systems, and business processes such as facility management. Due to their limited or lack of internet access, SCADA-type systems may appear to be more secure, but they too are vulnerable to cyber threats.

"Airline Security" refers to the techniques and methods used in protecting passengers, staff and aircrafts which use the airports from accidental/malicious harm, crime and other threats. Airline security threats could be by Hijacking, Cargo security, Aircraft Communications Addressing and Report System (ACARS) hacking, sabotage, cyber-attack,etc. However, "airline security" can be breached through cyber-attacks due to the following factors:

i. ACARS Hacking: ACARS hacking happens when hackers take over air traffic control transmissions and give pilots bogus orders. They could create a bogus flight plan update, create bogus weather, create fake message from plane to ground.
ii. Security threat On-board the Aircraft: Security threat on-board aircraft by cyber criminals is a new concern today. With modern days handheld smart digital devices being allowed on-board aircraft, Wi-Fi being made available to passengers, cyber security has become talk of the moment. In May 2015, Chris Roberts, a

26. Sinha, S. K. (2016, November 29). Security Aspects in Aviation Sector. Retrieved December 14, 2017, from https://in.linkedin.com/in/sanjeev-sinha-pmi-pba-5a7b392
27. In 2009, a truck driver managed to accidentally mess with the navigation systems of New Jersey's Newark airport as he drove past on a neighbouring highway.
28. For example – Incident noted in ICAO 12th Air Navigation Conference - Three software engineers were accused of disrupting operations at a new terminal at an airport in June 2011. They worked for a sub-contractor and when they didn't get a pay rise they sabotaged the program code. Check-in services failed 3 days later, and 50 flights were delayed, causing knock-on delays elsewhere.

prominent hacker, told the FBI that he had managed to make an aircraft “climb” and move “sideways” after infiltrating its in-flight entertainment system.

iii. Flight Management System Hacking (FMSH): FMSH too have been a target of cyber-attack. This, and attack on other airline systems have risen recently. An incident as recent as June 21, 2015 when LOT Polish Airlines was forced to cancel 10 flights scheduled to depart from Warsaw’s Chopin airport after hackers attacked its ground computer systems. The attack left the company unable to create flight plans for outbound flights, grounding around 1400 passengers.

iv. Remote Hijacking: It is an app that manipulates the Aircraft ACARS, which can give access to the plane’s flight management system (FMS). One can communicate with ACARS through hacking the airline’s systems or using a special radio.

v. Distributed-denial-of-Service (DDoS): DDoS attacks have grown in popularity to carry out a range of malware injection activities. Within such attacks, hackers utilize botnets of compromised networks to flood air traffic control and other critical systems with traffic, which results in a crash of the platform. Attackers may also ask for a ransom amount from the authorities to prevent disruption of flight management and control systems.

vi. Through Public Interfaces-Smart Phones: Through a Samsung Galaxy and a specially crafted app called Plane Sploit an airplane’s computer can be hacked remotely. Another example could be a new theory with Malaysia Airlines flight MH370 vanishing that a framework of malicious codes, triggered by a mobile phone, would have been able to override the aircraft’s security software.

vii. Mobile Applications: Most of the airline companies now provide Mobileapplication for airline services. This could be an opportunity for hackers for acyber -attack.

viii. Through Public Interfaces – Websites: Another public interface that could be vulnerable to cyber-attack is websites of airline companies. In a very recent incident (March 2015) it was reported British Airways' air-miles accounts, the coding site GitHub and the work chat service Slack have all been hit in the latest wave of cyber-attacks. User reported their account had been used by someone else to book a hotel room in Spain that their list of transactions showed "ex-gratia" deductions that had wiped out their entire credit, etc.

ix. Electronic Data Exchange Issues: The paper checks and balances that exist within the clerical world are not possible with EDI. While rare, the possibility that data will be intercepted and stolen or altered in transit does exist. Messages also may be deliberately or mistakenly duplicated. This can result in overcharges, wasted resources, and damaged relations between trading partners.

x. GDS/CRS Hacking: There have been incidents in past where hackers have gained access to airlines computer reservation systems. In one of the past incidents, O’ BRIEN from Boston, US, without authorization, accessed the computer reservation system at a travel agency by entering through the company's website, and intentionally sending commands cancelling ticketed airline reservations for approximately 60 passengers, thereby causing damage and a loss in excess of $96,000 to the travel agency. The unauthorized intrusion resulted in approximately 60 passengers being stranded at airports during the Christmas holiday season.

xi. Hacking via on-board Wi-Fi systems: The US Government Accountability Office (GAO) report said that modern aircraft that have the ability to access the internet through on-board Wi-Fi systems face the very real threat of being hacked. “A virus or malware planted in websites visited by passengers could provide an opportunity for a malicious attacker to access the IP-connected on-board information system through their infected machines,” according to the report.

b) **Legal Mechanism in curbing Cyber Crimes**

i. International Civil Aviation Organization (ICAO): The Chicago Convention 1944 (also known as the Convention on International Civil Aviation), established the ICAO, a specialized agency of the United Nations charged with coordinating and regulating international air travel. The civil aviation at global level is governed by the Convention 1944 along with various international conventions starting from the Warsaw Convention 1944 till the Cape Town Convention, 2001 which were ratified by member States. Annex 17 to

the Convention on International Civil Aviation speaks of the "security" i.e. safeguarding international civil aviation against acts of unlawful interference but unfortunately the threat posed by cyber-security was left unaddressed until recent times. Recently, the Universal Security Audit Programme commenced the auditing of access controls and related security lapses in ICT systems. This was the first step forward in identifying the potential risks in cyber security.

ii. International Air Transport Association (IATA):IATA has also provided guidelines for cargo security and cyber-security. For cyber-security IATA has put in place a three pillar strategy to address the cyber-security threat. They are; work to understand, define and assess the threats and risk of cyber-attack, and advocacy for appropriate regulation and mechanisms for increased cooperation throughout the industry and with and between Government agencies.

iii. Computer Emergency Response Teams (CERT):CERT is expert group that handle computer security incidents. It focuses on security breach and denial-of-service incidents, providing alerts and awareness campaign and engages in research aimed at improving security systems. The goal of Air CERT is to provide a capability to discern trends and patterns of intruder activity spanning multiple administrative domains.

c) **Cyber-security and Emerging LegalIssues:** Aviation industry provides the safest and the fastest transport system in the globe. Airports are increasingly data driven and rely upon accurate and timely information for efficient operations. However, increased reliance on data and increased integration also increases the risk of malicious cyber-attack that disrupts airport operations. In preserving the efficiency, security and resilience, the stakeholders should seriously consider the cyber threats. To strengthen the cyber-security, propositions made by experts and agencies globally must be adhered. Some of the challenges pertaining to cyber-security are; introduction of strong systematic tests against cyber-threats; critical systems should be tested by external and independent companies that have a real expertise in cyber security; provide high security for critical communication systems; setting up a real cyber-security culture in the critical entities of this sector; assessment and awareness of vulnerabilities; deep understanding of the threats and the risks involved are to be sorted out at a war footing; implement stronger internal policies and plans within the sector; setting up of legal framework by governments in terms of cyber-security; and finally the ICAO, ACI and the IATA must take stringent steps in resolving the cyber breach in aviation sector.

Conclusion

In the present days of globalization, where every State is competing towards economic development through the tools of civil aviation, yet global aviation industry remains a target for adversaries seeking to make a statement or cause substantial loss to person and property. Like many emerging threats, cyber-attacks still loom in the periphery, and are seen more as a stylized fiction than an actual possibility. The development of a stringent cyber-security framework is the need of the hour. The only way to tackle this new and emerging threat is to find a global solution. Every State has to come forward in tracing and tracking the cyber criminals at the root level instead at the fruit level i.e. after occurrence. Cybercrime should not become a "new cold war" nor should result in complete social chaos. If these cyber-security threats are not curbed, one has to re-think over the retaining of airports in opting one among the Conventional Airports or E-Airports or the Intelligent Airports.