# CYBER-SECURITY IN CIVILAVIATION: A REVIEW OF LITERATURE

**Prof. (Dr.) Kanwal DP Singh**
*Professor, USLLS, GGSIPU, Delhi*
E-mail : kanwal.als@gmail.com

**Dr. Jitender Loura**
*Dy. Director (DGCA), Govt.of India*
*& ResearchScholar, USLLS,GGSIPU,Delhi*
E-mail : jloura.dgca@gmail.com

***ABSTRACT***

*Civil Aviation is necessarily a critical infrastructure in any member state of ICAO Council.With the development of Civil Aviation infrastructurein the form of modern Airports, Data and Radar based Air Traffic Control, modern state of art aircrafts enabled with Wi-Fi systems, fly-by wire systems etc., enough opportunities are side by side available to the hackers to have unauthorized access to the data which they otherwise are not authorized to access. There has been tremendous increase in Cyber-attacks on the Civil Aviation critical Infrastructure in the recent decades. This paper seeks to review the literature in Cyber -security with respect to Civil Aviation Critical Infrastructure. For this purpose, the literature available after 2014 has been collected, analyzed and a systematic review of literature has been presented.*

**Keywords:** *Cyber-Security, Civil Aviation, Literature Review*

## 1. INTRODUCTION

Cyber Security in aviation has become an important issue in the recent decades due to overwhelming dependence on data, which is susceptible to hacking. Not a single segment of aviation is untouched from cyber threats, be it an airline operator, airport operators, ANS Providers, aircraft manufacturers and MROs (Maintenance Repair and Overhaul organizations). It is high time that the aviation cyber security policies and laws be meticulously followed by all stakeholders in letter and spiritin order to prevent cyber-attacks on Civil Aviation. In over last two decades, airport security have undergone sea change. From normal check-in to self- check-in kiosks, electronic flight display boards, Wi-Fi at airport and in air, in- flight entertainment system etc. which in turn has created opportunities for the hackers to enhance cyber-attacks .

Cyber security has recently emerged as a vital issue in air traffic control systems, the functionalities of which are seen to rely quite heavily on

communications that transpire between the networked agents situated in such systems (Heere 2016). Owing to the fact that current ATC systems have avoided incorporating mechanisms that are designed specifically for the protection of the cyber security of such systems, potential cyber-attacks along the lines of computer virus, false data injection and GPS spoofing could pose a serious threat to safety of such air control systems (Ellis and Mohan 2019). Systems for air traffic control are vulnerable to severe attacks via the internet and intrusion-detection capabilities need to be well established for the detection of potential cyber penetrations. Attackers are capable of taking full advantage of the software vulnerabilities that are characteristic of commercial IP products for the purpose of exploiting ATC systems, something that appears to be quite worrisome in a situation where nations of the world are faced with an increasing number of threats from state or nation sponsored cyber-attacks which, for the most part are executed with a remarkable degree of sophistication and finesse (Kim 2015). Hackers can for instance compromise FAA computers, and use such computers as channels for the acquisition of illegal access to information that is personally identifiable on employees working in the aviation industry (Bourgois et al. 2018). Critical network servers can also be seized control of by hackers, who in the process of doing so will gain the power that is required for shutting the servers down. An occurrence such as this can seriously end up disrupting the mission support network. More often than not, cyber-attacks are capable of spreading from mission support networks to national air security networks owing to the existence of system interconnections (Suciu et al. 2019).

## 2. OBJECTIVE

The objective of this research paper is to collect, analyze and review the literature available in the field of Cyber- Security in the context of Civil Aviation.

## 3. LITERATURE REVIEW

The focus of this article is to review literature pertaining to Cyber-Security in Civil Aviation comprising of all the segments viz., Airlines, Airports, Air Traffic Control (ATC), aircraft manufacturers and Maintenance, Repair & Overhaul Organizations (MROs). For this purpose, the literature after 2014 has been collected, analyzed and a systematic review has been presented.

### A. CYBER SECURITY IN AVIATION INDUSTRY OF SUB SAHARAN AFRICA

Lekota and Coetzee (2019) have analyzed cyber security in the context of the aviation industry of Sub Saharan African countries. It is argued by Lekota and Coetzee (2019) that cyber- attacks have taken place in the aviation community of Sub Saharan Africa several times in the years between 2016 and 2018 such as cyber-attacks for

financial gain, spying, terrorism and attempts by hackers for the identification and exploitation of vulnerabilities. What makes managing cyber-attacks a challenge for countries in Sub Saharan Africa, in the view of Lekota and Coetzee (2019), is the fact that information security mechanisms and frameworks that are required for coping with the significant rise in cyber-attacks are not in any given way, standardized. Lekota and Coetzee (2019) make the argument that in order to be ahead of such evolving cyber-attacks both outside as well as within the organization, responsibility has to be shared among aviation industry participants for securing aviation systems.

## B. IMPACT OF NEXT-GEN AIR TRAFFIC CONTROL ON AVIATION SECURITY

Weiland and Wei (2018) have evaluated the impact that the air traffic system of the Next Generation has on aviation security. Next-Gen as this is commonly known provides an outlet to the National Airspace System that operates digitally in the domain of cyber space. According to Weiland and Wei (2018) improvements in air traffic brought about by the Next-Gen system in addition to the risks associated with longstanding cyber-attacks in the information technology industry is something that has emerged as quite a challenging matter for air traffic management and the aviation community since cyber security challenges in this respect could impact greatly the assurance of security and safety that the Next-Gen system is seen to provide with regard to air transportation. Technological shifts that have taken place in the infrastructure of NAS , right from the conventional radar based systems to the present day networking systems is what demands a revision, re-definition and review of current regulations, standards and policies as well as norms for the purpose of reflecting as well as mitigating new risks. By engaging in an analysis of regulations, practices, standards, reports, and recommendations from industry and government, Weiland and Wei (2018) analyze security impacts and influences on Next-Gen, in addition to the risks that are associated with cyber security regulations and incidents in order to identify the most efficient and effective control measures that can be deployed over information systems in air traffic management, while providing direction to future research that can be undertaken in this area.

A review by Government Accountability Office (GAO) f the United States of America in 2015 found that many points were available to jump from networked computers to National Airport (NAS) systems. The review also showed that air traffic systems were terrible in patch updates and were not great at detecting network vulnerabilities and intrusions. All this makes things really much easier for hackers (Brandom, 2017).

## C. IOT COMPLEXITY AND THE RISK OF CYBER SECURITY

Horowitz (2018) has discussed the complexity brought about by the internet of things to commerce, homes and cities stating that theincrease in the risk of cyber security threats is a result of this complexity and further arguing that if such risks are to be reduced, resilient cyber-physical systems have to be formed that are capable of responding to various types of cyber-attacks or disturbances.

## D. CYBER SECURITY, AVIATION AND THE DEVELOPING LAW

Wood and Capone (2017) have studied the inter-relationship between cyber- security and aviation with special reference to the laws that are applicable in this respect. Wood and Capone (2017) define cyber security as a measure that is undertaken for protection of information systems from attacks that are unauthorized. It is the argument of Wood and Capone (2017) that advancements in technology and the fact that the internet is becoming all pervasive in nature have contributed to an increase in the concern for information security, stating specifically that there is no industry in the globe that is immune from or devoid of such concerns. The authors make use of the term cyber-attack to describe malicious activities that are directed at information systems or computers stating that the combined costs associated with such attacks as well as the corresponding defense measures happen to be quite significant. Wood and Capone (2017) argue that cyber security appears to be a greater concern for the aviation rather than any other industry in the world largely due to the fact that this is an industry that depends greatly on internet connectivity and computer technology. The research provides an overview of the problem of cyber -security in civil aviation and discusses the developing law in this matter that includes a discussion of both statutory and common law standards and regulatory activities.

## E. AIR TRAFFIC CONTROL SYSTEMS AND REGULATORY FRAMEWORKS

Andreades et al. (2017) have studied air traffic control systems and legacy avionics. The authors describe the Next- Gen air traffic system in detail and also draw up a list of potential issues pertaining to cyber security as well as associated cyber security incidents and anecdotes. Andreades et al. (2017) provide an overview of the regulatory framework as implemented in the commercial or civil aviation industry with introduced cyber security solutions and measures being well summarized by the authors.

Rusko and Finke (2016) by using speech analysis designed not only a safe Air Traffic Control System but procedure to verify the safety of system.

Government Accountability Office (GAO) of United States said in information security report of 2015: "The Federal Aviation Administration (FAA) is taking steps to protect air traffic control systems from cyber-based and other threats. Despite such measurements, some significant security control weaknesses remain. These vulnerabilities also seriously threaten the agency's ability to ensure the safe and uninterrupted operation of the national airspace system (NAS). In addition to control weaknesses or inadequacies, some shortcomings in border protection controls between less secure systems and the operational NAS environment also increase the risks associated with these weaknesses" (GAO, 2015).

## F. CYBER SECURITY, AVIATION AND ICAO

Abeyratne (2016) has carried out research on cyber security in the aviation sector with special reference to ICAO (2016). The research alludes to the use of a term, "cyber-jacking" which may be equated with the act of hijacking an airplane in the domain of cyber security and through the implementation of cyber technology. According to Abeyratne (2016), cyber- jacking can take from both outside a plane or from its inside. What acts as a catalyst in such a situation, in the view of Abeyratne (2016), is the increasing use on the part of airline passengers of internet connectivity that is used for playing games or watching videos and listening to music on board the aircraft. This research also makes mention of internet signals that are routed via existing communications architecture, a good example in this respect being ADS-B (Automatic Dependent Surveillance-Broadcast) or ACARS (Aircraft Communications Addressing and Reporting System). Both such systems are information communication systems as a result of which both can be vulnerable to cyber-attacks. The research goes onto state that there have been one or more than one attacks on computer systems of commercial airlines, after which the role that is played by ICAO (International Civil Aviation Organization), an international body that plays a leading role in preventing cyber terrorism from taking place, is elaborated upon, accompanied by constructive recommendations on how cyber security can be suitably enhanced and improved.

## G. CYBER SECURITY POLICIES, CYBER ESPIONAGE IN USA& UK

Stoddart et al. (2016) have studied cyber security policies as practiced in the USA and UK. A comparison is made of cyber security arrangements in both these countries by virtue of the fact that both countries happen to be liberal democracies. The research outlines the supervisory control as well as data acquisition systems as implemented in the US and the UK after which UK and US policies with respect

to cyber security have been analyzed in detail. A wider discussion of cyber-crime and the cyber espionage system is entered into, with the argument being made by Stoddart et al. (2016) that national approaches to breach of CNI and other aspects of cyber security have to be internationally concerted while also acknowledging at the same given time that the concerns and needs of civil society and private industry ought to be taken into consideration.

## H. CYBER SECURITY AND THREAT TO SAFETY CRITICAL SYSTEMS

Johnson (2016) has analyzed the growing threat that exists to cyber security pertaining to safety critical systems. As argued by Johnson (2016) common vulnerabilities have been created as a result of introducing commercial and off the shelf software products across aviation, maritime, power generation infrastructures as well as rail. Johnson (2016) emphasized the urgency of moving beyond various types of high level policies for addressing the many engineering challenges that presently threaten cyber security as applicable with regard to safety critical systems.

## I. AIR & SPACE LAW AND CYBER SECURITY

Kaiser and Mejia Kaiser (2015) have studied cyber security with reference to air and space laws. It is argued by Kaiser and Mejia Kaiser (2015) that cyber security is a term that encompasses technical measures that require a regulatory framework for adequate implementation and that this is a regulation that needs to be incorporated into laws dealing with air and the virtual space in timely fashion, at a time when technology is still in a stage of progress. The research elaborates on regulatory frameworks and legal principles that deal with cyber security in the context of air as well as space law.

## J. CYBER SECURITY IN SMART AIRPORTS

Lykou et al. (2014) have undertaken research on cyber security in smart airports and have discussed the controls and measures that are undertaken here for the purpose of threat mitigation as well as cyber resilience. The authors state that airports are the forerunner in all types of technological innovation owing to the fact that air travel passengers are exponentially increasing in number with every passing year. Consequently, airports are seen to enhance infrastructure intelligence on a regular basis, and have been evolving slowly and steadily as smart facilities for supporting growth, thereby providing customers with a truly enjoyable and comfortable not to mention efficient travel experience. However, it pointed out by Lykou et al. (2014), that there are new challenges that aviation must adapt to and deal with today, such as integrating industrial IoTs (internet of things) in all airport facilities

accompanied by the increasing use of computers, smart phone devices, tablets on the part of employees and passengers. As a result, it is argued by Lykou et al. (2014) that cyber security is gradually emerging as a key enabler when it comes to ensuring passenger safety. Smart airports are making an effort to provide customers with optimal services in a manner that is both sustainable as well as reliable, and this is achieved by working around domains such as security, safety, efficiency and growth. The research undertaken by Lykou et al. (2014) discusses the implementation rate associated with cyber security measures as undertaken in major commercial airports, risk scenario analysis of malware attacks related to the internet of things along with actions to mitigate threats in this respect and it also discusses the malicious threats that are seen to evolve owing to the smart devices installed as well as IoTs (internet of things). The aim of the research undertaken by Lykou et al. (2014) is to ensure development of robust security governance and enhancement of operational practices in smart airports, and this is done by presenting a comprehensive and systematic analysis of the types of malicious attacks that are seen to occur and which are likely to occur in smart airports, facilitating airport communities to comprehend such risks and act proactively by engaging in the implementation of resilience measures and best practices with regard to cyber security.

## K. AIRCRAFT MANUFACTURERS

Modern aircraft manufacturers have enabled aircrafts with latest technologies, Wi-Fi system, Fly-by-wire system etc. to reduce weight, enhance passenger comfort and reduce cost which in turn induces a lot of cyber-security risks by introducing data to the hackers through malicious code, BOTS/ BOTNETS etc.

Airbus industry, one of the biggest commercial aircraft manufacturers, on an average is hit by at least 12 cyber- attacks per year, mostly in the form of ransom ware.

Stander & Ophoff (2016) proposes steps that aircraft manufacturers initiated to avoid occurrence of cyber- security incidents in regard to an aircraft.

## L. MAINTENANCE REPAIR AND OVERHAUL ORGANIZATIONS (MROS)

According to Higgins (2017), the Department of Homeland Security of United States of America identifies the following areas of aviation as susceptible to Cyber-attacks, viz.,

- Air traffic control
- Global positioning systems
- Information technology infrastructure
- Operations
- Maintenance, and other unknown threats

- Wireless networks

Costanza & Prentice (2018) found that MROs are susceptible to cyber-attacks through supply chain a owing to global reach, lack of international standardization in cyber-security, round- the-clock operations and most importantly its own unpreparedness.

Costanza & Prentice (2018) put forward through Oliver Wyman's MRO Survey that only 41% of airlines, 9% of MROs and 50% of OEMs, have supply chain security standards.

Anton (2017) observed that MROs are prone to attacks in software installations during lifecycle of an airplane's by airlines, MROs andOEMs, and in digital data throughACARS (aircraft communication, addressing, and reporting system) data and maintenance data.

## 4. GAPS IN THE LITERATURE REVIEWED

While the literature that has been reviewed above points to cyber security policies and control measures as deployed in various countries of the world with respect to the aviation industry in general and the air traffic control system in particular, and talks about the mitigation techniques that need to be deployed in order to suitably control and combat the threat of cyber security in aviation, little mention is made of the type of laws and legal frameworks that can be utilized for this purpose (Simmons 2017). New research must therefore be conducted on the impact that laws pertaining to cyber security can have on aviation operations (Lykou et al. 2019).

## V. RESULT AND CONCLUSION

Cyber-attacks on the critical infrastructure have recent origin due to over dependence on data. The literature that has been reviewed pertains to almost all the segments of Civil Aviation. The reviewed literature points to Cyber- Security policies and control measures as deployed in the member states of ICAO, There is a shortfall in the implementation of Cyber- security policies uniformly owing to disparity in resources, inapt security measures and inadequate infrastructure. New Research may be conducted on the impact of laws on Civil Aviation Operations as well as a comparative study between the nations with developed infrastructure as well as Cyber security polices and the developing nations may be conducted.Further research may be conducted in one specialized segment of Civil Aviation viz, Airline, Airport or Air Traffic Control and the positive, negative or neutral impact of cyber security laws on that sector may be analyzed.

## REFERENCES

[1] Abeyratne, R., 2016. Aviation Cyber Security: A Constructive Look at the Work of ICAO. *Air and Space Law*, *41*(1), pp.25-39.

[2] Abeyratne, R., 2019. Regulating Cyber Security. In *Legal Priorities in Air Transport* (pp. 157-194). Springer, Cham.

[3] Andreades, C., Kendrick, J., Poresky, C. and Peterson, P., 2017. *Cyber Security in Civilian Aviation: Insights for Advanced Nuclear Technologies*. UCBTH- 17-001, Berkeley, CA

[4] Anton, J. (2017). Cyber-Security; an EASA perspective on developments and challenges. Retrieved from https:// www.iata.org/whatwedo/workgroups/Documents/ Paperless_Conference_2017/ Day1/1100-1130_Cyber-Security_ EASA.pdf

[5] Bourgois, M., García, E. and Hullah, P., 2018. Air traffic management and air navigation service providers. In *The Routledge Companion to Air Transport Management* (pp. 60- 80). Routledge

[6] Costanza, D. & Prentice, B. (2018). MRO survey 2018:
Tackling industry disruption. Retrieved from https:// www.oliverwyman.com/content/ dam/oliverwyman/v2/ publications/ 2018/ april/ MRO-Survey-2018- web.pdf

[7] Dodge, M. and Kitchin, R., 2018. The challenges of cyber-security for smart cities. In *Creating Smart Cities* (pp. 205-216). Routledge.

[8] Ellis, R. and Mohan, V. eds., 2019. *Rewired: Cybersecurity Governance*. John Wiley & Sons.

[9] GAO, (2015), http://www. gao.gov/assets /670/668169.pdf accessed June 06, 2021.

[10] Heere, W.P., 2016. Bibliography of Air Law 2015. *Air and Space Law*, *41*(4), pp.397-415.

[11] Higgins, J. (2017). DHS' Manfra details efforts to secure aviation sector from cyber attacks. Inside Cyber-Security. Retrieved from https: //search.proquest.com. ezproxy.libproxy.db.erau.edu/ docview/1963863433?accountid =27203

[12] Horowitz, B.M., 2018, March. Policy Issues Regarding Implementations of Cyber Attack Resilience Solutions for Cyber Physical Systems. In *2018 AAAI Spring Symposium Series*.

[13] International Civil Aviation Organization. (2016). Addressing Cyber-Security in civil aviation. Retrieved from https:// www.icao.int/Meetings/a39/ Documents/WP/wp_017_en.pdf

[14] Johnson, C.W., 2016. Why We Cannot (Yet) Ensure the Cybersecurity of Safety-Critical Systems. http://eprints.gla.ac.uk/ 130822/

[15] Kaiser, S.A. and Mejia-Kaiser, M., 2015. Cyber Security in Air and Space Law. *ZLW*, *64*, p.396.

[16] Khatoun, R. and Zeadally, S., 2017. Cyber-security and privacy solutions in smart cities. *IEEE Communications Magazine*, *55*(3), pp.51-59.

[17] Kim, K., 2015, August. Cyber security considerations for designing IoT-based control systems. In *International Workshop on Information Security Applications* (pp. 288-299).
Springer, Cham

[18] Lekota, F. and Coetzee, M., 2019. Cyber-security Incident Response for the Sub-Saharan African Aviation Industry. In *International Conference on Cyber Warfare and Security* (pp. 536-XII). Academic Conferences International Limited.

[19] Lenders, V. and Martinovic, I., 2019. Surveying Aviation Professionals on the Security of the Air Traffic Control System. In *Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6-7, 2018, Revised Selected Papers* (Vol. 11552, p. 135). Springer

[20] Lykou, G., Anagnostopoulou, A. and Gritzalis, D., 2014. Smart Airport Cyber-security: Threat Mitigation and Cyber Resilience Controls. *Sensors*, *19*(1), p.19.

[21] Lykou, G., Iakovakis, G. and Gritzalis, D., 2014. Aviation Cybersecurity and Cyber- Resilience: Assessing Risk in Air Traffic Management. In *Critical Infrastructure Security and Resilience* (pp. 245-260). Springer, Cham

[22] McAndrew, I.R. and Vishnevskaya, E., 2018, July. Is the Sky Above us Safe and How Has This Been Influenced by the Past and Present Policies?: Unmanned Aerial Systems and their Cybersecurity Implications. In *2018 9th International Conference on Mechanical and Aerospace Engineering (ICMAE)* (pp. 435-439). IEEE

[23] Rusko M. and Finke, M. (2016), "Using speech analysis in voice communication: A new approach to improve air traffic management security," 2016 7th IEEE International Conference on Cognitive Info-communications (CogInfoCom), Wroclaw, , pp. 000181-000186.

[24] Simmons, H.O., 2017. Cyber- security in Aviation: Constant Vigilance Required. *J. Air L. & Com.*, *82*, p.771.

[25] Stander, A. and Ophoff, J (2016) Cyber security in civil aviation.

[26] Stoddart, K., Jones, K., Soulsby, H., Blyth, A., Eden, P., Burnap,

P. and Cherdantseva, Y., 2016. Live free or die hard: US–UK cybersecurity policies. *Political Science Quarterly*, *131*(4), pp.803-842.

[27] Strohmeier, M., Niedbala, A.K., Schäfer, M., Lenders, V. and Martinovic, I., 2018. Surveying Aviation Professionals on the Security of the Air Traffic Control System. In *Security and Safety Interplay of Intelligent Software Systems* (pp. 135-152). Springer, Cham.

[28] Suciu, G., Scheianu, A., Petre, I., Chiva, L. and Bosoc, C.S., 2019, April. Cyber-security Threats Analysis for Airports. In *World Conference on Information Systems and Technologies*(pp. 252-262). Springer, Cham.

[29] Urban, J.A., 2017. Not Your Granddaddy's Aviation Industry: The Need to Implement Cyber- security Standards and Best Practices within the International Aviation Industry. *Alb. LJ Sci. & Tech.*, *27*, p.62.

[30] Weiland, L.V. and Wei, G., 2018. Evaluating the impact of Next Gen's air traffic system on aviation security. In *MATEC Web of Conferences* (Vol. 189, p. 10030). EDP Sciences.

[31] White, J., 2016. Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. *Global Security Studies*, *7*(4)

[32] Wood, S.A. and Wallace, M.S., 2017. Aviation and Cyber-security: AN INTRODUCTION TO THE PROBLEM AND THE DEVELOPING LAW. *The Brief*, *46*(4)