RESEARCH REVIEW JOURNALS
Volume-03
Issue-12
December -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Perceived Cyber Threats to Aviation Industry in India

[1]Anjan Kumar Sinha, [2]Dr Nikhil Kulshestra & [3]Dr Binod Kumar Singh

[1]Research scholar, COMES,UPES Dehradun (India)
[2]Associate Prof (HR &OB),COMES,UPES Dehradun (India)
[3]Assistant Prof (Statistics & Design),COMES,UPES ,Dehradun (India)

ARTICLE DETAILS

Article History
Published Online: 10 December 2018

Keywords
Aviation industry, cyber attacks, cyber security

ABSTRACT

World over it is progressively helpless against cyber-attacks due to interruptions that influence the respectability of data. This failure is an element of world economy which is quiet substantial. Aviation sector contributes to 7% of World GDP and Indian Civil Aviation close to 9%, thus any disruptions can cause huge losses. Another muddling factor is the thickness of India's cyberspace, which does not allow a uniform legitimate or specialized limit for data protection laws. Security threats to civil aviation have turned out to be more challenging due to cyber-physical systems and their integration. One of them is that it is seeming considerably more confounded and advanced to oversee is cyber-attack. Today, the worldwide civil aviation network is depending on Information Technology (IT) frameworks. Apart from these issues, due to primarily based oppressor attacks on airplane and air systems, air terrorism carries the threats to aviation sector across the globe. There is a need to be certain degree of awareness of the situation by the environment. The Aviation ecosystem in India must get down building multiple layers of secured firewalls in order to remain safe and overpower the menace of cyber threats and Cyber terrorism. IT frameworks will be a key driver of development and proficiency, including frameworks to upgrade safety and security. In this paper an effort is made to highlight the cyber security threats in the civil aviation industry to Indian subcontinent and the solution for limiting them.

1. Introduction

India's increasing digital economy has the world's second largest client-based internet. The Union government's led activities like 'Digital India', and the accentuation on governance based ondigitizationis increasing the nation's data framework. It is possible that the honesty of India's cyber platforms will progressively be exposed to threats and endures vulnerabilities in future. Around the world, cyber security has long gone up against desperation because of the virtual financial system developed over the previous decade in comparison to previous years. Besides, the significance of cyber security keeps on developing every day with the rise of cyber-physical systems that make up the Internet of Things including, "smart" devices for the home.However, against this setting of digital change, achievable that both the public and private area is neglecting to maintain pace with cyber security threats. The sadness of the prevailing manner to deal with tending to cyber security is apparent within the news features. In the preceding years, various corporations around the world have succumbed to each nation and non-nation programmersare surely understood organizations, for example, Target, Sony, and HSBC, bringing about a great many records about users being uncovered [1]. For whatever duration of these negative externalities are not tended to, the non-public quarter will spend short of what should on cyber security India's key test in cyberspace stems from outer threats as well as the structure and thickness of its digital environment. While technology is moving from the West toward the East, data is flowing in the turnaround heading, offering law authorization organizations couple of alternatives to ensure and, where justified, extricate the data of Indian residents. The abroad care of data additionally uncovered the data of natives powerless against remote attacks: for example, database situated in outside soil yet facilitating the data of Indian residents be attacked by an outsider, Indian specialists have constrained purview to explore and arraign the culprits. While a National Cyber Security Agency or a Cyber Command would offer institutional, between agency architecture to collaborate, safeguard and react to attacks on Indian foundation, a more extensive vital system is required to ensure Indian resources abroad, both civilian and key. This makes an appraisal of India's vital advantages in cyberspace and proposes a framing cyber security policy and operational zing its key goals. Such architecture must show as a National Cyber Security Agency, a pinnacle command association at the national level [2].

A. Civil Aviation in India

The Indian aviation industry is several the worlds' fastest developing industry. It has experienced tremendous changes following the enhancements of the aviation industry in India. When possessed by the Government, the aviation sector of India is presently claimed as private with full service airways and moderate transporters. Relatively 75% of the local aviation sector comprises of the private airlines. Earlier saw as exorbitant methods for transportation, managed, benefited by numerous. The aviation area has been the maximum imperative fragment within the economic development of a country. It assumes important working transferring individuals or devices starting with vicinity then onto the subsequent, it is domestic or international, particularly while the separations covered a long way [3]. Hardened contention and perfect sports of the Government of India added gasoline to make bigger the two flights and fleets, Air Deccan changed into the leader airline, which provided low duty to the residential and in addition worldwide desires and made some other landmark in aviation area in India. Currently, standard residents could

without much of a stretch access the aviation service from their individual air terminals. In an exceedingly aggressive condition, the management of superb services to passengers is the center upper hand for an airline's benefit and supported development. In the previous decade, as the air transportation advertises has turned out to be more difficult, numerous airlines have swung to concentrate on airline service quality to build service fulfillment. Service quality conditions impacts a company's upper hand by holding client support, which thus results in development in piece of the pie. Conveying superb services to passengers are fundamental for airline survival, so airlines need to understand what passengers anticipate from them.

B. Cyber Vulnerability of Aviation

In aviation, there are numerous functions of attack for cyber terrorists/hackers; from the maker of aircraft and its hardware, to any phase of their project. 'Cyber terrorism, irrespective of whether or not led through humans, organizations or states, May be the digital structures of companies, which is designed and built in equipment and programming in airports, air traffic manipulates systems; It could be the goal organizations related to the development of plane and components that they are used for civil or military functions'. Airplanes are systems of building [4]. It entails a complex system of segments that basically include, but are not confined to a base structure, communication connections, sensors, and avionics. Ground manipulates structures, air direction carrier providers, and extra communication joins supplement this. By 2020, ADS-B17, a reconnaissance technology will supplant radar as the essential methods for following aircraft and will be a mandatory prerequisite on the dominant part of aircraft. It's going to supply passengers and climate facts, providing better verbal exchange among the plane and air traffic manage. The ADS-B structure stays unprotected and defenseless in opposition to cyber-attacks. Communications amongst aircraft and air traffic controllers stay decoded and unbound, making it open for attacks that may disappointed air passengers. It remains helpless in opposition to sticking and satirizing of information.

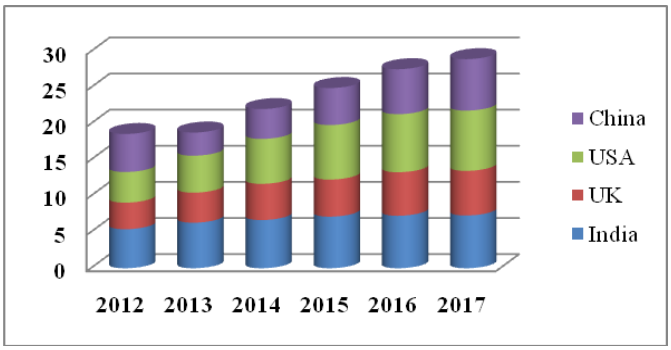

Figure I: No. of Increasing Cyber Threats in Civil Aviation

Table I: Vulnerability areas in the aviation security

Air traffic Controller	Airport Operations Centre	Passenger Baggage Screening	Runway Lighting, HVACS (Heating Ventilation & Air-conditioning)
Airport Terminals	Aircraft Maintenance Agencies	Ground Service Transportation	Employees
Wi-Fi Systems	BYOD (Bring your own Devices)	OEMs (Original Equipment Manufacturers)	Supply Chain logistics
Flight Entertainment Systems/Avionics	Passengers	Cargo Operations	Mobile phones

2. Major threats to the aviation industry

The American Institute of Aeronautics and Astronautics (AIAA) called for cyber security threats refers to the international business aviation

industry. James Albaugh, AIAA President and a previous best official at Boeing, says cyber threats ought to be considered important for business aviation and recommended that a coordinated methodology should be taken. On August 13, the AIAA formally released a decision paper entitled "A structure for Aviation Cyber Security", plotting existing and increasing cyber threats to the commercial aviation mission and paying attention to the absence of global concession to cyber security in aviation. There is no regular coordination of endeavors looking for a global management

A. Air Traffic Control

Air Traffic Control (ATC) is polishing off extra automatic and much less physically supervises. The accelerated usage of Unmanned Aerial Vehicles (UAVs) has raised issue over verbal exchange between ground manipulate stations and aircraft. Solutions are Internet-based and ultimately present new cyber security problems, offering the arena to new vulnerabilities that did not exist which could jeopardize civil aviation protection and productivity. The ATC framework is powerless to attack – a few security analysts unveiled in groups, as an instance, DEF CON and Black Hat that they might misuse vulnerabilities within the structures. The Automatic Dependent Surveillance-Broadcast (ADS-B) has been a noteworthy goal for White Hat hackers speaks on the groups, Brad Haines as an example, who guarantees that the framework is decoded and unauthenticated. 'Phantom is in the Air (Traffic)' introduction that suggests how ADS-B may be exploited and suggests manager of the framework using a Smartphone

B. Aircraft

The maximum current aircraft development, the potential for cyber vulnerabilities while Commercial Off-The-Shelf (COTS) programming and device solutions are delivered into aircraft components, increasing risk, interconnected systems that permit conversation of all fashionable air traffic instructions amongst ATC and the aircraft, Aircraft directors: An accelerated exchange of official communication with the aircraft builds its vulnerability.

C. Airlines: Website and Networks

The threats contain risks to web packages, for example, the Sykipot backdoor device, which collects facts and might harm the companies; or the abuse of Twitter debts which can hurt the organization's infamy. The industry is also a goal for politically persuaded cyber-attacks.

3. Cyber security and civil aviation

Aviation is one of the world's most essential organizations. The development of the industry over the previous decades has made it one of the motors for the extension of the worldwide economy. The aviation industry has driven a generous piece of the financial and social coordination that has brought a significant part of the world closer. By moving billions of passengers and billions of large amounts of cargo every year, the industry has changed the lifestyle of people. Transportation security turned into a national issue since 1931 in the United States. As indicated by the FAA (1986), the primary aviation hijacking occurred in Arequipa, Peru on February 21, 1931.

As it has in numerous other complex human exercises, the uses of ICT in civil aviation has increased exponentially over late years, from the development of aircraft to communications and route instruments, alongside every one of the thousands of organizations that interface the different parts of an airport. As in different fields, the digitalization and management online of such complex instrumentation have presented significant issues related with cyber security [5]. It isn't amazing then that a 2012 report by the British Center for the Protection of National Infrastructure (CPNI) found that the interface and relationship to ICT-utilize has raised the vulnerability of aircraft and aviation systems, and subsequently the effect of inevitable bargain. Notwithstanding financial and managerial development, it stays clear that shortcomings connected with cyber movement represent an imperative threat to civil aviation.

Table II: Motivation of threats and its resources

Threat	Resources	Type	Goal/Motivation
Passive Observers	None - Very low	Passive	Information collection / Financial or privet interest
Script Kiddies / Hobbyists	Low	Active	Any major impact / Thrill and popularity
Cyber Crime	Medium - High	Active	Maximizing effect / Financial profits the usage of e.g., blackmail or valuable information
Cyber Terrorism	Low - Medium	Active	Political or non-secular motivation / Massive disruption and casualties
Nation State	Unlimited	Active	Weapons / Targeting specific, probably navy devices

Source: McAfee 2016 Threats Predictions

Civil aviation has been a particularly appealing target. As the sector has developed, the threats issuing faces, have changed in both measurement and methodology, far from customary physical attacks on aircraft and airports to new sorts of occasions that incorporate the various cyber threats. The aviation industry faces Increase issues passengers' control structures, to the plane, to the airline agencies and airports and fringe intersections. The recognized threats originate from the prevailing concept of aviation industry structures that are interconnected and reliant.

A. Cyber security challenges for the aviation industry

As the aviation industry is known for giving one of the most secure kinds of transportation, it is mandatory to consider the cyber threats if they need to protect the effectiveness, security and flexibility of their systems. To manage these threats and to keep up a high level of certainty, partners would need to proceed with the endeavors. To strengthen cyber security, the aviation industry must consider a portion of the recommendations made by specialists. The accompanying recommendations appear to be the most suitable:

- ✓ The aviation industry needs to develop and to present strong ordered tests against cyber threats notwithstanding the consistence testing officially executed. Inside security testing, it is then neglected because of its inward requirements and an absence of aptitude. It is more than imperative to test every one of the segments autonomously and the entire systems by outside experts. These experts would have the preferred standpoint to be autonomous, less obliged, unprejudiced, inventive, and more than everything else master in breaking systems.

- ✓ The aviation industry is comprised of customary disconnected systems that are increasingly associated and uncovered (AIAA, 2013). Like in different organizations, for any venture it is essential to:
  - Survey the requirements and the recompense for these outside connections
  - Guarantee that security forms are actualized
  - Guarantee that vulnerabilities can be tended to rapidly
  - Know that security updates may break current confirmation. The decision of uncover and interface separated systems suggests to consider another condition [6]

- ✓ Provide high security for basic communication systems, for example, the Radio and Television. This security ought to guarantee strong validation, classification, respectability and accessibility. Some other unprotected communication systems ought to be considered at last, it is vital to observed that basic and non-basic systems are detached.

- ✓ Any organization in the aviation industry should bring issues among every one of the workers on the significance of considering cyber threats. It is vital to

set up a genuine cyber security culture in the basic elements of this industry [7].

- ✓ Every organization in the aviation industry ought to survey in term of cyber security. These organizations ought to know about their vulnerabilities and execute a few measures to decrease them. Like some other industry, the aviation sector ought to consider cyber security as they improve the situations HR, Finance, tasks etc.

- ✓ Implement more grounded inside strategies and plans inside the organization. To be sure, as organizations depend on computer-based systems associate with different organizations or people, for example, passengers; it is mandatory to reinforce interior managements and plans.

- ✓ It would be vital to actualize additionally recuperation plan and to build versatility.

- ✓ Governments should set up a few directions and standards in term of cyber security

4. Air traffic control surveillance

With the end goal to exhibit more clearly how aviation needs to manage the changing cyber security threat, this phase indicates an earlier generation: air passenger's surveillance [9]. The management of advances use is basic to the protected task of airspace, yet as it turns out to be more technologically propelled, it additionally turns out to be more unreliable. This change is illustrative of flying technology. All through this segment, we survey the development regarding our threat demonstrated as shown in Table III. From this, we endeavor to coordinate which systems are 'in reach' of a given attacker, which is summarized in Table IV.

Table III: Summary of Surveillance Technologies

Technology	Ground/Air Dependent	Cost	Deployment Status
PSR	Ground	High	In use
SSR	Ground	High	In use
TCAS (STANDARD)	Air	Moderate	Mandate by 2015
TCAS (HYBRID)	Air	Moderate	Optional
ADS-B	Air	Low	Mandate by 2020
WAM	Ground	High	In deployment

Source: Ablon, Libicki, and Golay, 2014

Table-III explores the abilities of the distinctive threat specialists and the surveillance systems that are important to them, further assessing the conceivable expense of the required equipment [9]

Table IV: Overview of Attacker Capabilities

Threat Agent	Capabilities	Hardware / Cost	Systems of Interest
Passive Observers	Eavesdropping, use of website & mobile apps.	Internet access, $10 SDR receiver stick	ADS-B, Mode S
Script Kiddies / Hobbyist	Eavesdropping, replay, assaults denial of service.	COTS SDR transmitter, $300-$2,000.	ADS-B, Mode S
Cyber Crime	Resources for big-scale operations with state-of-the-art transponders.	Directional antennas, small UAVs with SDR transmitters, $5,000-$10,000.	ADS-B, Mode S
Cyber Terrorism	Resources for specific high-effect operations, though commonly on a restrained scale	As with cybercrime but potentially on a smaller, more targeted scale.	ADS-B, TCAS, Mode S
Nation State	Anything bodily and computationally viable.	Military-grade radio equipment, capability for electronic warfare	Any ATC system

Source: IATA, Oxford Economics

5. Conclusion

Tending to the cyber security threats would require an important realignment of ways government has moved toward this difficulty and stable authority to overcome existing commercial region and government's issues and explore the limits that have observed. Given the significance of cyber security to the digital financial system, nations should join up to confront these problems and make another worldview for constructing resilient systems. Barrier, along these lines, must not be the sole variable considered, since an entire investigation should likewise incorporate the evaluation of attackers' technical skills. Civil aviation authorities have recognized fear-based oppressor associations, activists and cyber criminals as representing the critical threat to that sector.

The technical aptitude of cyber criminals will keep on enhancing in the coming years. Constantly expanding on the web bootleg market will be a motivation to develop complex tools. Although their potential for access to technical skill makes it important to observe for these on-screen characters, it is additionally implausible that cyber criminals will permit targets, for example, air traffic control systems to occupy them from

significantly more profitable and less unsafe targets, for example, the commercial and financial divisions of civil aviation. There are exercises to be gained from such a methodology: the proposed National Cyber Security Agency (NCSA) is prefaced on the rule that while cyber-attacks may not be completely frustrated, they can in any event be more precisely anticipated through continued insight collects.

References

1. B. Elias, Airport and Aviation Security. CRC Press, 2010.
2. B. Elias, Securing General Aviation. Congressional Research Service, March 3, 2009.
3. ICAO (2002) DOC 8973 Restricted - Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference, Annexes to the Convention on International Civil Aviation, ICAO, Montreal, Canada, 2002.
4. P.Nečas, B. Lippay, S.Szabo, Barack H. Obama´s view on global security: a shift in the US foreign and security policy? In: Strategic impact. - ISSN 1841-5784. - No. 2 (39) (2011), pp. 113-118.
5. D. BuhaliseAirlines: Strategic and tactical use of ICTs in the airline industry 2003
6. The Current State of Cyber Security Readiness in the Aviation IndustryVolume 1: Matter of Time and MoneyAuthor: Sion Camilleri. September, 2014
7. A. Costin, A. Francillon Ghost in the Air(Traffic): On insecurity of ADS-B protocol and practical attacks on ADS-B devices.
8. H. Teso Security Research Team Aircraft Hacking Practical Aero Series April 2013
9. Fontana, J.A., Iyengar, S.S., Pitchford, A.R., Smith, N.R. and Tolbert, D.M., Unisys Corp., 2000. Software system development framework. U.S. Patent 6,167,564.

