



# Cyber Threat Landscape: The Aviation Industry

<b>Sector:</b>	Aviation
<b>Global Oversight:</b>	International Civil Aviation Organization (ICAO), International Air Transportation Association (IATA), Airport Council International (ACI), Civil Air Navigation Services Organization (CANSO), International Coordination Council of Aerospace Industries Associations (ICCAIA)
<b>Top Aircraft Suppliers:</b>	Boeing Co, Airbus Group SE, United Technologies Corp, Lockheed Martin Corp, Honeywell International Inc, Mitsubishi HI Ltd, General Dynamics Corp, Northrop Grumman Corp, Raytheon Co, BAE Systems. <sup>1</sup>
<b>Future Concerns:</b>	Modernization of the Air Traffic Management Systems: NextGEN, SESAR; Drones; Geopolitical instability; Terrorism.

## Executive Summary

The aviation industry is accustomed to dealing with threats to safety that can come from a variety of sources such as human and mechanical failure, adverse weather, or even geopolitical factors. As the airline industry and its supporting infrastructure continues to modernize, exposures to cybersecurity threats also increase. This expanding cyber attack surface must be considered to maintain industry safety expectations.

Past attacks on the airline industry have come from

notable APT groups, cybercriminals, and even hacktivists. Details about these attacks offer insights into the motivations, tools, and operating techniques used by attackers. These insights are made more valuable when applying them to future technological changes in the industry and knowing how these new technologies may be abused by attackers.

This document explores some of the existing and future concerns around cyber threats to the airline industry. Some recommendations are also provided.

<sup>1</sup> <https://www.statista.com/statistics/264366/revenue-of-the-worldwide-leading-aircraft-manufacturers-and-suppliers/>

## The Aviation Industry

The aviation industry comprises the creation, operation and use of aircraft within earth's atmosphere. It includes all elements of innovation, manufacturing and supply for airlines as well as the business operation of airports and air traffic management. The aviation industry overlaps somewhat into the aerospace industry. However, the aerospace industry embraces the design, manufacturing and operation of transportation beyond earth's atmosphere, including rockets, space stations and satellite systems. Globally, airlines service more than three billion passengers a year and 50 million tons of freight, contributing approximately \$664.4 billion to global GDP. According to "Aviation Benefits Beyond Borders," this is over half of the size of the global financial industry<sup>2</sup>. IATA reported that passenger numbers are expected to increase to 4.3 billion in 2017 (a growth of 6%) and a rise in cargo to 62 Million tons (a growth of 4.%). Historically, aviation security referenced issues such as: unlawful seizure of aircraft; destruction of aircraft; hostage-taking; forced intrusion of aircraft or at an airport; weapons or material intended for criminal purposes. However, the industry has had to adapt to new challenges as it faces an increasing number of targeted and opportunistic cyber-attacks.

## The modernization of Aviation

The aviation industry has experienced a great deal of modernization and is currently undergoing some important transformations. This has led to a number of new risks despite increasing operational efficiency. The evolution in design of aircraft has increased the dependency on software, which has helped to take the complexity away from the pilot in the cockpit. There are multiple sensors within the aircraft that provide the pilot with situational awareness. The drive towards smarter aviation has increased the attack surface providing more opportunities for actors to find a pathway for an attack<sup>3</sup>. The same data-heavy and technology dependent trajectory can be seen in airports.

The U.S.A. under the proposed NextGen project is attempting to improve upon legacy radar systems with Automatic Dependent Surveillance — Broadcast (ADS-B) technology. ADS-B uses GPS satellites and enables greater accuracy than radar and can be used where radar coverage is difficult<sup>4</sup>. The success of this technology requires aircraft to have implemented the correct avionics, an arrangement of satellites and a ground network of stations to transmit aircraft information. The ADS-B system allows for aircraft-to-aircraft communication. NextGen is also updating analog to data communications which will supplement Voice-Over-IP (VOIP) for air traffic controllers. Tower services are in operation at 56 airports in the USA already. Europe is utilizing the same technology in their initiative SESAR Joint Undertaking 2020. The SESAR solutions catalogue for air traffic management stakeholders outlines a solution for ADS-B combined with a Wide Area Multilateration (WAM) system<sup>5</sup>. These two projects are also addressing emerging challenges such as the rapid increase in the use of drones. The concern is that ADS-B was never designed to be secure, instead it was built for function and to account for the forecasted growth in air traffic. ADS-B equipment does not support encryption<sup>6</sup>.

Researchers have investigated the vulnerabilities within ADS-B systems for a few years now. Because of the lack of encryption, there are concerns that a man-in-the-middle attack is possible or that flight plans can be spoofed, leading to mid-air collisions. The Federal Aviation Administration has been devising methods for verifying authenticity. The use of multilateration is a system that accounts for Time Difference of Arrival (TDOA), which can help to determine and filter spoof flights<sup>7</sup>.

## Drones

Looking beyond the military and personal use of drones, commercial application of drone technology is on the rise. Commercial uses for drones, or Unmanned Aerial Systems (UAS), range from construction sur-

2 <https://aviationbenefits.org/economic-growth/value-to-the-economy/>

3 [https://resources.sei.cmu.edu/asset\\_files/Webinar/2015\\_018\\_100\\_447930.pdf](https://resources.sei.cmu.edu/asset_files/Webinar/2015_018_100_447930.pdf)

4 [https://www.faa.gov/nextgen/where\\_we\\_are\\_now/nextgen\\_update/progress\\_and\\_plans/adsb/](https://www.faa.gov/nextgen/where_we_are_now/nextgen_update/progress_and_plans/adsb/)

5 [http://www.sesarju.eu/sites/default/files/solutions/SESAR\\_Solutions\\_Catalogue\\_Ed2\\_2017.pdf](http://www.sesarju.eu/sites/default/files/solutions/SESAR_Solutions_Catalogue_Ed2_2017.pdf)

6 <https://securityintelligence.com/ads-b-and-aviation-cybersecurity-should-passengers-be-concerned/>

7 <https://www.ainonline.com/aviation-news/aviation-international-news/2012-09-03/ads-b-insecure-and-easily-spoofed-say-hackers>

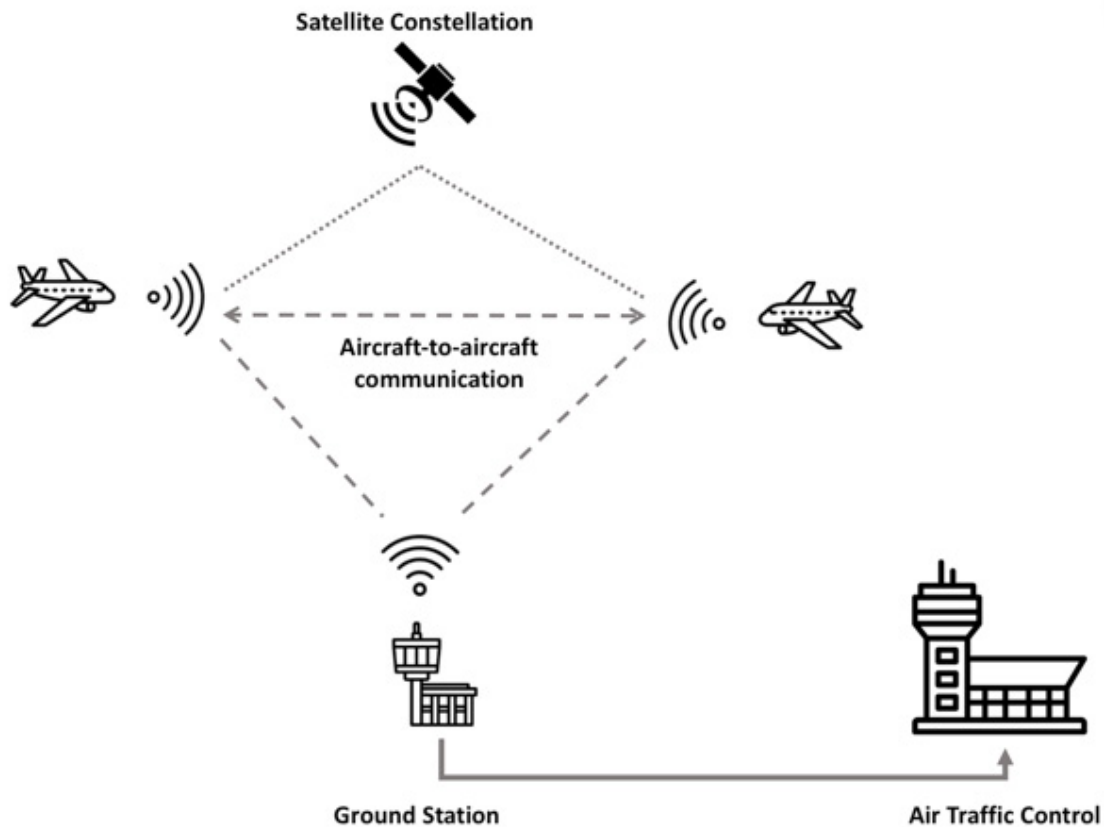


Figure 1 ADS-B Technology

veying to damage assessments for insurance to crop monitoring for farmers<sup>8</sup>. Future UAS uses could include product delivery or even taxi services although these innovations are likely some years away. UAS integration with air traffic control for flights in controlled airspace is expected in the next 2–5 years. The growth of UAS technology for commercial applications will eventually garner greater interest from criminals, terrorists, and APT groups alike. This will be an area to watch for new threats.

## Past attacks and campaigns

### Advanced Persistent Threats

Approximately 30 APT groups have been reported to have targeted the aviation and aerospace sector<sup>9</sup>. Most

of these groups have been attributed to China including APT1-10, APT12, APT14, APT16-19, APT22, APT24-27 and APT31<sup>10</sup>. This has been in alignment with China's strategic requirements and for the modernization of China's air force. More recently, Iran was attributed to threat group APT33. FireEye reports that spear-phishing emails were sent to employees whose jobs related to Aviation and the group registered multiple domains masquerading as Saudi Arabian aviation companies. The companies spoofed were: Boeing, Alsalam Aircraft Company, Northrop Grumman Aviation Arabia and Vinnell Arabia<sup>11</sup>. It is suspected that the purpose of the attack was to gain insight into a joint venture and reveal Saudi Arabia's aviation capabilities<sup>12</sup>. Iranian threat group OilRig also targeted an Israeli airline Israir, impersonating the company in a malicious excel file

8 <https://www.mckinsey.com/industries/capital-projects-and-infrastructure/our-insights/commercial-drones-are-here-the-future-of-unmanned-aerial-systems>

9 FireEye accounts for 27 in report dated 2013, not including the activity conducted by Russia in Ukraine under APT28, and recent activity from APT31 and APT33.

10 <http://www.zdnet.com/article/china-targets-aviation-industry-to-spy-and-steal-industry-secrets/>

11 [https://cyber-peace.org/wp-content/uploads/2017/09/Insights-into-Iranian-Cyber-Espionage\\_-APT33-Targets-Aerospace-and-Energy-Sectors-and-has-Ties-to-Destructive-Malware-%C2%AB-Threat-Research-Blog\\_-FireEye-Inc.pdf](https://cyber-peace.org/wp-content/uploads/2017/09/Insights-into-Iranian-Cyber-Espionage_-APT33-Targets-Aerospace-and-Energy-Sectors-and-has-Ties-to-Destructive-Malware-%C2%AB-Threat-Research-Blog_-FireEye-Inc.pdf)

12 <https://news.sky.com/story/state-backed-iranian-hackers-target-aviation-sector-11044880>

sent to victims<sup>13</sup>. Operation Cleaver, also attributed to Iran and reported by Cylance, provides details of victims in aerospace and aviation spanning multiple countries including: China, Qatar, Israel, Pakistan, Saudi Arabia, South Korea, UAE and the USA.

Because the industry forms part of the Critical National Infrastructure, targeting aircraft and associated systems including suppliers and manufacturers are increasingly likely in the midst of intensifying geopolitical tension. Russia's attacks against the Boryspil International Airport and Ukraine International Airlines is an example of this<sup>14</sup>.

### Cybercrime

Frequent flyer account points and hotel points are sold in underground markets. Cybercriminals look to steal credentials and account information which can be exchanged for gift cards or even be cashed out<sup>15</sup>. Phishing lures can also use these themes to entice users and grant criminals opportunistic access to sensitive information.

### Hacktivism

Airlines have been the subject of attack in hacktivist campaigns because of their relationship to the nation state. In 2016, flight screens at Vietnam's major airports were defaced with critical messages regarding Vietnam's claims in the South China Sea<sup>16</sup>. Japan's two primary airports were the target of denial-of-service

attacks during #Opkillingbay by Anonymous because of Japan's dolphin hunting<sup>17</sup>. Airline websites are also the target of opportunistic defacement as can be seen by the following image taken from zone-h.org<sup>18</sup> (fig.2).

### Threats to Aviation

There are a myriad of vectors that actors can choose from, as the industry is exposed to a number of data-dependent operations. The diagram below provides a high-level view of some of the areas that are important to the successful operation of a flight and where attackers can leverage these critical areas. For example, on board an aircraft the network can be segregated into three domains; closed, private and public domains<sup>19</sup>. These account for the following areas:

- Closed: for the control of the aircraft and satellite communication
- Private: flight operation and maintenance, such as the cabin crew area
- Public: for inflight entertainment systems and passenger connectivity.

However, these areas are not always effectively separated, as researcher Chris Roberts demonstrated when he used the in-flight entertainment system to hack into the flight controls system. Roberts claimed to have been able to monitor traffic in the cockpit and cause one of the airplane engines to climb<sup>20</sup>. Hugo Teso, another security researcher with a background as a commercial











2018/01/22	djava.hattab	R		starsky-airlines.pl//images/jd...	Linux	mirror
2018/01/08	ifactoryx	M		anket.ulsairlines.com/fx.html	Win 2008	mirror
2017/12/29	RxR	M		airlinefiles.com/king.php	Linux	mirror
2017/12/29	mindless injector	M		airlineticketsagent.com/mind.php	Linux	mirror
2017/12/27	TEAM_CC	M R		turkishairlines.com/gray.txt	Linux	mirror
2017/12/25	Kadd3chy	H		www.loyaltyairline.sr	Linux	mirror
2017/12/23	GAZA	M		find-cheap-airline-tickets.com...	Linux	mirror
2017/12/11	Zedan-Mrx			airlinesociety.in/OwNed.html	Linux	mirror
2017/12/03	ifactoryx	M		pegasusairlines.com/fx.html	Win 2008	mirror
2017/11/28	BD GREY HAT HACKERS	M		www.airlinerreservation.us/dead...	Linux	mirror

Figure 2: zone-h.org defacements of airline websites

13 <http://www.clearskysec.com/oilrig/>  
14 <https://www.scmagazineuk.com/ukraine-blames-russia-for-cyber-attack-on-airport/article/531367/>  
15 [http://online.wsj.com/public/resources/documents/secureworks\\_hacker\\_annualreport.pdf](http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf)  
16 [http://www.defence.gov.au/ADC/Publications/documents/digest/Spring\\_2017/IPSD\\_Cumming\\_spring2017.pdf](http://www.defence.gov.au/ADC/Publications/documents/digest/Spring_2017/IPSD_Cumming_spring2017.pdf)  
17 <https://www.scmagazineuk.com/anonymous-attacks-two-japanese-airports/article/535257/>  
18 Zone-h.org query using keyword "airline"  
19 <http://fhr.nuc.berkeley.edu/wp-content/uploads/2017/04/UCB-TH-17-001-Cybersecurity-in-Civilian-Aviation.pdf>  
20 <http://aptnnews.ca/2015/05/15/hacker-told-f-b-made-plane-fly-sideways-cracking-entertainment-system/>



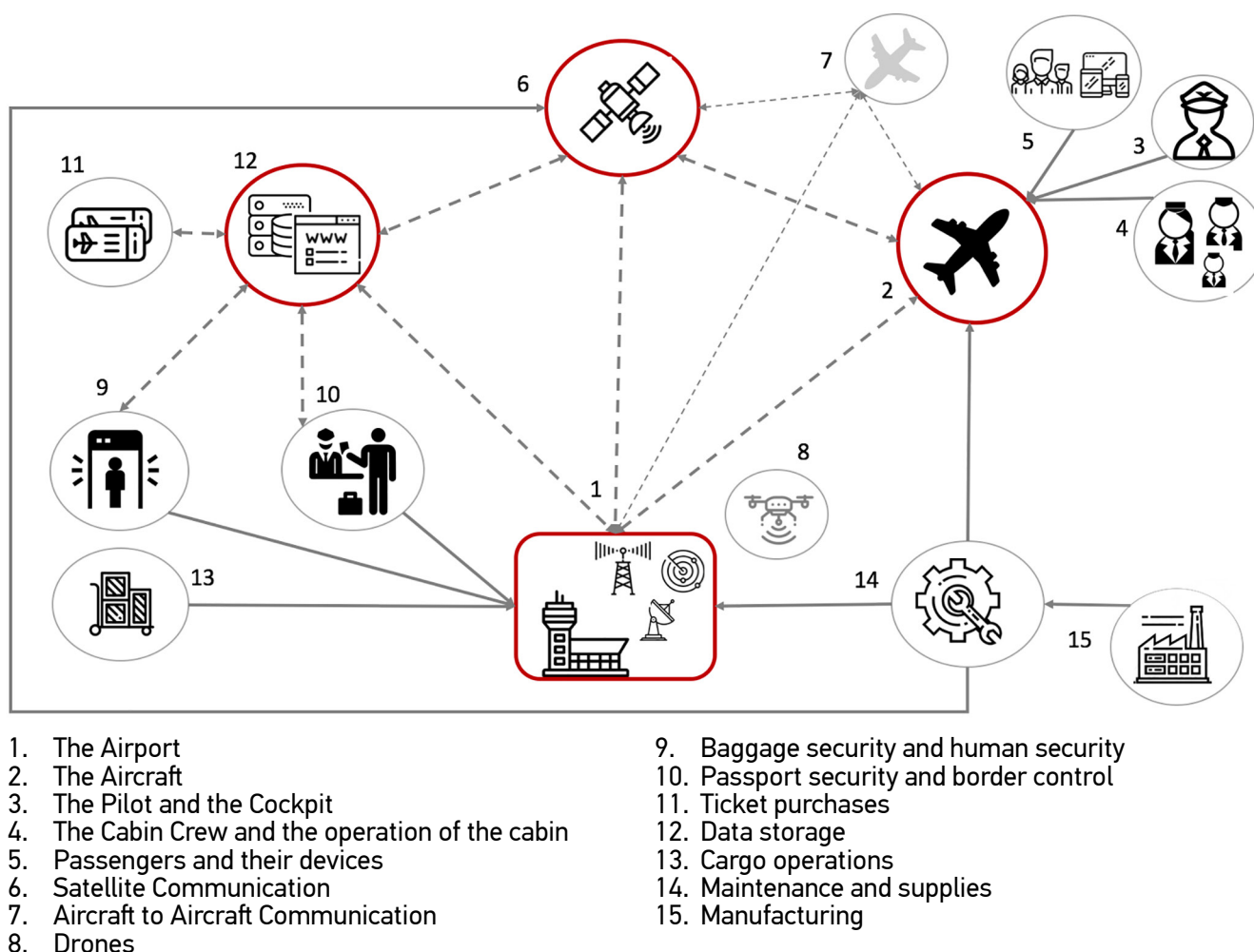


Figure 3: Visual Depiction of Commercial Airline Communications

pilot, explains that ADB-S can be used for reconnaissance as it is good for locating and pinpointing targets. He suggests that the Aircraft Communications Addressing Reporting System (ACARS), which is the “digital datalink” between aircraft and ground stations, can then be used for passive operating system fingerprinting and enumeration. Using this information, an actor can pursue an active exploration of which vulnerabilities exist to exploit. He also demonstrates that many airline products and software from manufacturers like Honeywell and Thales can be bought and examined on eBay<sup>21</sup>.

IATA conducted a broad research project called “Future of Aviation Industry 2035”. It brought together a number of industry specialists and partners to collaborate on what they considered to be key risk issues for the

industry. The research identified 50 “drivers of change” which were further categorized into 11 themes. Cybersecurity and Terrorism featured as the most popularly considered drivers of change, both of which feature within the “geopolitics” theme<sup>22</sup>. This research highlights how susceptible the industry is to national and international political changes and conflict.

## Conclusions & Recommendations

There have been many changes and advances in the airline industry in recent years but many more are coming. Each of these will present new challenges in terms of security and safety for the industry. Collaboration amongst industry players and investments in key personnel, tools, and tailored security solutions to address

21 <https://www.youtube.com/watch?v=wk1jKQvMx8>

22 <https://www.iata.org/policy/Documents/iata-future-airline-industry.pdf>

these challenges will ensure a safe march forward into new technological horizons.

## Recommendations

The following are broad recommendations that can help address the challenges of securing new and existing technology as discussed in this document. It is assumed that some or all of these suggestions may already be adopted in one form or another by members of the airline industry. They are included here merely as a means of providing holistic guidance crucial to securing complex systems such as those commonly found in the airline industry.

- Perform periodic threat modeling around new technologies and address key findings
- Ensure security is an integral part of the development process for any new technologies
- Allow vetted security researchers to access and test critical components and systems
- Continue to foster a rich spirit of collaboration amongst industry players
- Quickly share any new threats uncovered
- Stay abreast of changes in the threat ecosystem: new malware, techniques, actors
- Efficiently address vulnerabilities once they are known
- Develop mitigations for vulnerabilities that can not be easily or quickly addressed
- Consider impact of DDoS on systems and components and develop response plans