The Netherlands Press

Journal of Airline Operations and Aviation Management

Article

Is Safety Always Going to be More Important Than Privacy?

Tomasz Balcerzak[1*], Alexandra Yarushina[2], Jan Rajchel[3]

[1]Adjunct at Lazarski University in Warsaw, Faculty of Law and Administration, Poland.

E-mail: tomasz.balcerzak@lazarski.pl, Orcid id: https://orcid.org/0000-0002-3845-998X

[2]Student at Lazarski University in Warsaw, Faculty of Law and Administration, Poland.

E-mail: yarushinasasha@gmail.com, Orcid id: https://orcid.org/0000-0002-4684-2890

[3]Professor at University of Natural Sciences and Humanities in Siedlce, Poland.

E-mail: jan.rajchel@uph.edu.pl, Orcid id: https://orcid.org/0000-0001-7248-3863

DOI: https://doi.org/10.56801/jaoam.v2i1.3

Abstract.

Lately Elon Musk published headlines news that has been focused on his private jet and its whereabouts, leading the billionaire to announce he is taking legal action against a 20-year-old who has been tracking his travels. The US Federal Aviation Administration is proposing an upgrade to air transportation that will fundamentally overhaul the current, aging system. A key component, the automatic dependent surveillance broadcast (ADS-B) system, will enhance air traffic monitoring and control by requiring aircraft to continually broadcast position, identity and velocity via unencrypted data links to ground stations. Although ADS-B may enhance air traffic safety and support the increase in traffic demands, open broadcast of clear aircraft data points raise serious security concerns. The ability to encrypt ADS-B message transactions would afford protection to ensure that the confidentiality of aircraft data is not compromised. The implementation of an encryption framework for a large, distributed and dynamic system, however, is nontrivial. This paper discusses the ADS-B as a tool — the way that it is beneficial and the way it could be exploited.

Keywords: aviation safety, aviation privacy, aviation security, EUROCONTROL, ADS-B, Flightradar24, GPS.

Journal of Airline Operations and Aviation Management Volume 2 Issue 1

Received Date 08 April 2023
Accepted Date 25 May 2023
Published Date 15 August 2023

1. Introduction

Lately Elon Musk published headlines news that has been focused on his private jet and its whereabouts, leading the billionaire to announce he is taking legal action against a 20-year-old who has been tracking his travels. Jack Sweeney, the owner of the ElonJet account on Twitter, used public flight-tracking information to keep tabs on where Musk's jet was going, up until he was banned from the website. Musk's attempts to silence the account have only garnered it more attention, and it has no doubt captured the attention of those in the business aviation market.

But legal action to enable private jets to fly under the radar will be tricky to enforce, according to aviation law. Automatic Dependent Surveillance-Broadcast (ADS-B), which is being used to track the jets is necessary to ensure safe skies, so it's difficult to see how any legal action could allow its use to be side-stepped.

"Safety is always going to be more important than privacy," David Hernandez, shareholder at Vedder Price tells Corporate Jet Investor (CJI). "The harder it is to obtain ADS-B information, the harder it's going to be for someone to use it for its intended purpose for safety."

David Hernandez says that there is legislation in place to increase the level of privacy and security of ADS-B information, so that the only people able to track the flight data of private flights are specific individuals with licenses. However, there are loopholes around this that people are able to take advantage of. "You, me or anybody could go on Amazon and buy a receiver and an antenna and get that same information from anybody in the world, and that's what that guy is doing with Elon Musk," he says. "If he's banned from Twitter, he'll just switch to Instagram or Facebook or start his own web page, you can't stop him."

Keri Dowling, president, Air Law Office, agrees that it is a serious issue: "The real issue for people who own private jets and who are flying around to support their businesses, or their philanthropic endeavors, is security. A lot of these people go into the private aviation sector because of the level of security they need that just can't be met on commercial flights, so security is a huge concern."

Keri Dowling says there are programmes that the FAA has introduced to try to protect security, such as the Limiting Aircraft Data Displayed (LADD) and the Privacy Impact Assessment (PIA). These aim to help disguise the identity of those flying, although they can be bypassed. "The programmes have their limitations, which is how Elon Musk has been able to be followed, and it's of huge concern for my clients," says Keri Dowling.

Elion Musk claimed on Twitter that tracking his jet could lead to an "assassination", David Hernandez says there is another threat for companies; corporate espionage. "It's very important to many of my clients, particularly those in private equity, because they're involved in mergers and acquisitions," he says. "So people try to track many of my clients to see what cities they fly to, to determine whether or not they're going to buy a specific company. When you have a client in Pittsburgh all the time, and everyone knows that a company in Pittsburgh is up for sale, people may start trying to buy up the stock of that company." Traders can subscribe to a Nasdaq feed showing corporate flights.

So apart from spending $44bn to buy Twitter and close down the accounts that track you, what can owners do? Keri Dowling and David Hernandez advise their clients to look into options like setting up trust companies, using the LADD and PIA programmes to use code names rather than tail numbers and real names, and even advising people to fly by charter instead. Fractional ownership is also very private. No one knows who is flying by NetJets, Flexjet or Airshare for example.

The National Business Aviation Association (NBAA) has been working to make end-users aware of the risks to privacy and security, with advice on how to submit LADD requests on their site. Dan Hubbard, senior vice president of Communications at NBAA says no one should have to surrender their safety or security when getting on a jet. He says: "The need to allow for an opt-out from having your flight tracked and published in real time by anyone, anywhere in the world, with any motive and an internet connection, has long been recognized in bipartisan legislation repeatedly passed by Congress."

Keri Dowling adds: "Musk may have a very controversial name right now, but this will be closely followed by people like Jeff Bezos and George Soros and other people impacted by this ability to follow flights. It's something that's going to be very impactful on our industry."

2. Legal base and technology

Future civil aircraft are envisioned to depend on air-to-air and air-to-ground data communications for air traffic management. However, ease of access to wireless communications as well as the personal, political or proprietary nature of air travel raises privacy concerns for some aircraft users. A major concern is exploitation of aircraft's communications for deriving identity and position trajectories of that aircraft, resulting in potential privacy violations such as by helping to infer travel intent and profile places of interest. Privacy enhancement is however challenging to achieve due to a delicate balance with airspace security. This paper identifies location privacy threats and proposes anonymity solutions that can enhance privacy level of aircraft operators and passengers without compromising airspace security.

Existing Air Traffic Control (ATC) systems are at their life's end, with software, system architectures and communication links not having the growth capacity to meet demands of future aviation. The "e-Enabled aircraft" promises to help modernize ATC using advanced sensing, computing and communications, e.g., Global Positioning System (GPS), Automatic Dependent Surveillance Broadcast (ADS-B), Internet Protocol networking. In the European Union, Regulation (EU) 2020/587 has posited a mandate for ADS-B retrofitting, and the general deadline for all flights under Instrument Flight Rules had passed in 2020.

The ADS-B (Automatic Dependent Surveillance - Broadcast) system enables the presentation of the traffic situation in real time. The image obtained is similar to that seen on radar, but information about the position of the aircraft, calculated on the basis of the GPS signal, direction, altitude, flight number, etc., is propagated by devices mounted on the aircraft. In other words, each object communicates its position to everyone around it.

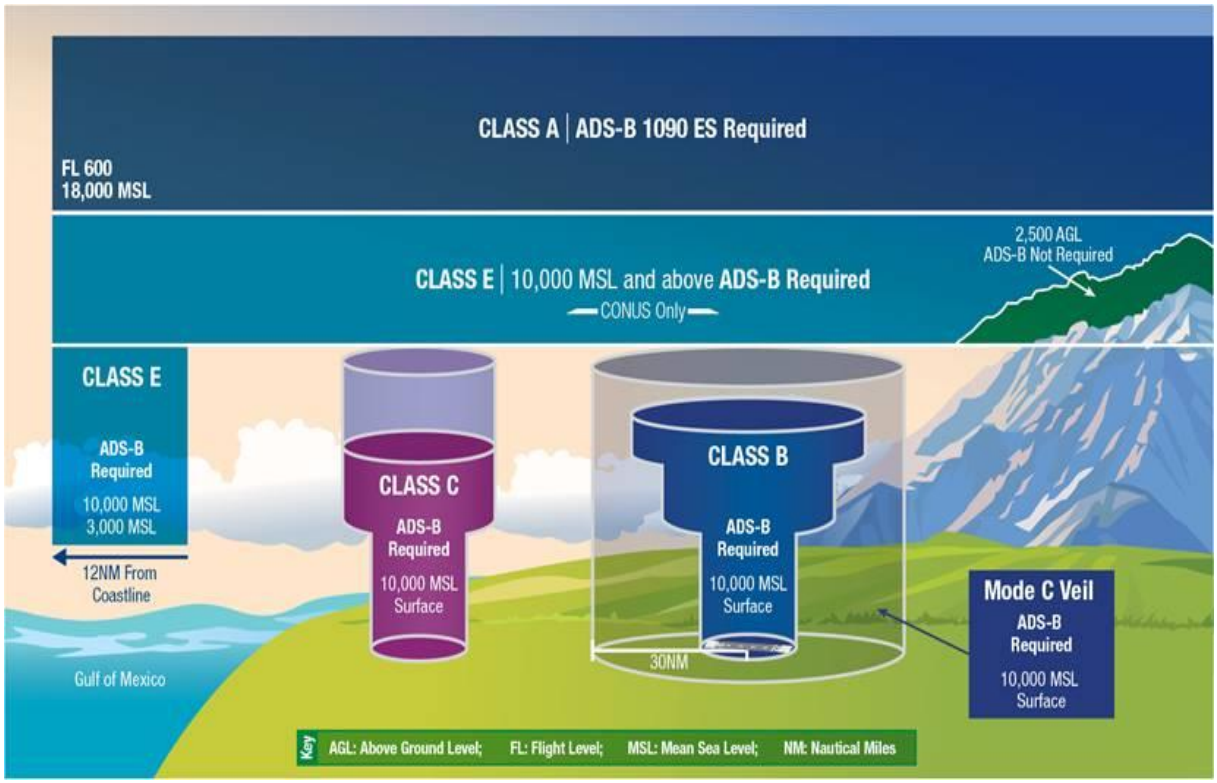

Figure 1. Automatic Dependent Surveillance - Broadcast (ADS-B)

Source: Automatic Dependent Surveillance - Broadcast (ADS-B), https://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afx/afs/afs400/afs410/ads-b, access: 05.04.2023.

Automatic Dependent Surveillance–Broadcast (ADS–B) is an advanced surveillance technology that combines an aircraft's positioning source, aircraft avionics, and a ground infrastructure to create an accurate surveillance interface between aircraft and ATC. ADS–B is a performance–based surveillance technology that is more precise than radar and consists of two different services: ADS–B Out and ADS–B In.

The receiver of the signal can be another device supporting the ADS-B system and therefore there is no need to use expensive and heavy radars. Each aircraft equipped with the ADS-B system and visualization screen has graphical access to the traffic situation.

The position read from the on-board systems together with the direction of flight, altitude, speed, flight number, is packed in a "package" and then propagated using the ADS-B system on frequencies 1030-1090MHz.

Initially, it was envisaged to introduce full data transmission in the 1030 MHz transmitting channel and the 1090 MHz receiving channel used by Mode-S transponders. Finally, the 1090 MHz channel is used to transmit information about the position and speed of the machine.

The data collected by the ADS-B receivers are not burdened with a large distance error (as it could be in the case of radars) and are not dependent on the terrain (the radar had to "see" the scanned object to correctly determine the

position). In addition, the ADS-B system transmission channel enables the transmission of other information: weather, field warnings, etc.

The abbreviation ADS-B is also expanded like this:

- A Automatic - The system is always on. No central management required;
- D Dependent - its accuracy depends on the quality of GNSS (Global Navigation Satellite System) position data, for example GPS, Galileo;
- S Surveillance - Allows surveillance, similar to radar view;
- B Broadcast - constantly spreading information.

Far different from radar, which works by bouncing radio waves from fixed terrestrial antennas off of airborne targets and then interpreting the reflected signals, ADS-B uses conventional Global Navigation Satellite System (GNSS) technology and a relatively simple broadcast communications link as its fundamental components. Also, unlike radar, ADS-B accuracy does not seriously degrade with range, atmospheric conditions, or target altitude and update intervals do not depend on the rotational speed or reliability of mechanical antennas.

In a typical applications, the ADS-B capable aircraft uses an ordinary GNSS (GPS, Galileo, etc) receiver to derive its precise position from the GNSS constellation, then combines that position with any number of aircraft discretes, such as speed, heading, altitude and flight number. This information is then simultaneously broadcast to other ADS-B capable aircraft and to ADS-B ground, or satellite communications transceivers which then relay the aircraft's position and additional information to Air Traffic Control centers in real time.

The 978 MHz Universal Access Transceiver ("UAT") variant is also bi-directional and capable of sending real-time Flight Information Services ("FIS-B"), such as weather and other data to aircraft. In some areas, conventional non-ADS-B radar traffic information ("TIS-B"), can also be uplinked as well.

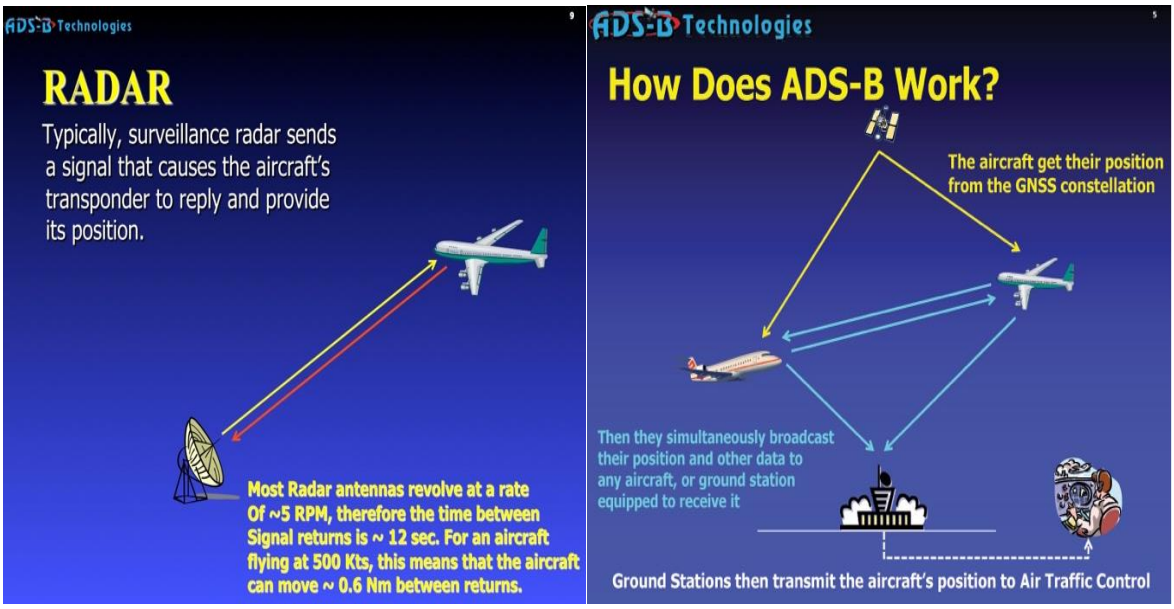

Figure 2. ADS-B Technologies working mechanism.

Source: http://www.ads-b.com, access: 05.04.2023

ADS-B will someday replace most of the World's Surface Surveillance Radars (SSR's) for routine Air Traffic Control functions. In the European Union, Regulation (EU) 2020/587 has posited a mandate for ADS-B retrofitting, and the general deadline for all flights under Instrument Flight Rules had passed in 2020.

3. ADS-B receivers on drones

ADS-B receivers will be in all DJI drones produced from 2020 New regulations for the use of drones will be introduced in the USA. One of the changes will be the obligation to mount receivers to identify the drone. The reasons for the introduction of ADS-B receivers (called Airsense in the case of DJI) and other improvements can be found in the presentation titled: "Enhancing Security: Protecting the Sky in the Age of Drones".

The ADS-B system allows drones to be displayed on the radar and control software. Therefore, in the case of flights of two drones in close proximity, operators receive information that a drone is also flying in their area. The position of this drone on the map is also visible as in a regular radar. In addition, various services will be able to easily identify the owner of any drone that weighs more than 250 grams.

In the presented document, we read that DJI has defined 10 basic goals that it will want to achieve in the near future:

- Installation of Airsense systems (ADS-B receiver) in all production drones over 250 grams from 2020;
- DJI is developing a new automatic warning for drone pilots flying over longer distances;
- DJI will establish an internal Safety Standards Group to meet regulatory requirements and customer expectations;
- The aviation industry needs to develop standards for reporting drone incidents;
- All drone manufacturers should install geofencing and remote aircraft identification;
- Governments must be able to remotely identify drones (Aeroscope).
- Governments must require knowledge tests for new drone pilots;
- Governments must designate no-fly or restricted areas;
- Local authorities must be able to respond to drone threats. (again, it's about the Aeroscope);
- State governments must step up their enforcement of drone operations. Brendan Schulman, Vice President of Policy and Legal Affairs at DJI also announced in Washington on May 22, 2019 that an important goal of the company will be to increase safety.

4. Concerned about privacy: the FAA provides the ability to block the display of private aircraft data

Since May 2010, when the US Federal Aviation Administration (FAA) announced that by January 2020 all ships operating in the airspace must be equipped with ADS-B transponders, the issue of installing ADS-B systems and mandatory positioning aircraft aroused much controversy at first. Government agencies such as the Pentagon, CIA, FBI and DHS (department of home security) have expressed concerns about the security and secrecy of certain flights. One of these concerns is that which is expressed by several high-profile persons who worry about the dispersal of data concerning the patterns of their air travel. Specifically, there stands a risk of inter alia breaching security, stalking,

releasing insights into mergers and acquisitions, defamation, doxing; some of these are serious criminal offenses that would be duly dealt with by the government body holding jurisdiction in case of factual violation.

Legal thought and the jurisprudence uphold the view that private individuals have less effective means for rebuttal than do public officials and public figures (Gertz v. Welch).

The US Federal Aviation Administration (FAA) has developed a plan to allow owners of ADS-B-equipped aircraft to disable real-time tracking of their flights. Although ADS-B is required from January 1, 2020 for all aircraft operating in US airspace, this fact has caused some aircraft owners to worry about the transparency of the transmission of this data - especially location - over the internet. While being in the public eye is a result of one's choice of enterprise or image, it is important to remember that these risks may affect the family and children of high-profile persons. Nonetheless, some of the risks listed above are consequences of nondiscriminatory internet access (Regulation (EU) 2015/2120) and freedom of expression (ECHR Art. 10), both of which are rights on an equal level as the right to privacy (ECHR Art. 8). The ethical quandary of competing rights is in some situations dealt with by allowing case-by-case exceptions, implementing further regulations and, better yet, the creation of highly-specific programs. The FAA has demonstrated an example of each.

In July 2019, under a separate agreement with government entities, the Federal Aviation Administration allowed government aircraft to operate with ADS-B disabled. "Unbroadcast" flights are authorized by the FAA upon prior notification by the entity concerned.

To ensure operator safety and privacy, the FAA will enter into new agreements with flight tracking service providers that will restrict data sharing if requested by aircraft owners.

For this purpose, the agency is to create a special Internet portal, where it will accept applications from people who want to block information about the location and identification of their aircraft in real time. It is intended that only organizations authorized by the FAA, such as law enforcement, will have access to this data.

According to Ed Bolen, president and CEO of the National Business Aviation Association, the lack of a privacy solution "has discouraged some operators from equipping themselves with ADS-B. "No one should give up privacy and security just because they're getting on a plane," he explained.

Previously, aircraft owners who wanted to block the display of their aircraft data could submit a Block Aircraft Registry Request (BARR). This program was subsequently renamed Limiting Aircraft Data Displayed (LADD) . The purpose of LADD is to allow aircraft owners and operators to request that their aircraft is filtered out from the feeds of internet flight tracking vendors. The vendors in question are subscribers to the System Wide Information Management (SWIM) . SWIM is an accessible telecom service, which acts an amalgamation of information relevant to aviation, including NOTAMs, meteorology, terminal data, en route automation, etc. In cases when the FAA determines that a flight tracking service provider willfully violates the terms and displays more than permissible under the program,

the Agency may suspend or stop providing data to that company through SWIM. There is no requirement to join the program that is based on the principle of nationality. The legal basis for establishing understanding is the Data Access User Agreement. Finally, the program does not exclude or limit data from the oversight of the FAA itself.

Another program authored by the FAA is called Privacy ICAO Address . The PIA program enables interested aircraft owners to request an alternate, temporary ICAO aircraft address, which will not be assigned to the owner in the Civil Aviation Registry (CAR). The PIA program holds more requirements to its users while providing privacy from even individual-use ADS-B receivers. The requirements to participate in the PIA are that the aircraft be U.S. registered, 1090 MHz ADS-B equipped, using an obtained third-party call sign and flying in domestic U.S. airspace. Therefore, it can be said that the PIA is its in experimental stage. Perhaps, if it is fully developed and quantitative in its benefit one day, it will be endorsed by ICAO.

As was stated earlier, access to SWIM is available based on a subscription — a fact which suggests that the lawfulness of the public's observance of civil aviation minutiae is not in question, and that, on a typical day, no harm is foreseen by willful transparency. Notwithstanding, the same information is not minutiae for pilots, who make operational and safety decisions based on it. The moment that there is an irregularity, such as the internal breakdown of the NOTAM system in January of 2023, or external interference, such as the 2022 cyberattacks on U.S. airports and the 2015 cyberattack on LOT Polish Airlines' ground computers, the aviation network is paralyzed. To provide the bigger picture, cyber-attacks reported to or identified by EUROCONTROL's EATM-CERT (European Air Traffic Management Computer Emergency Response Team) rose by 530% between 2019 and 2020 . While the previous examples concern attacks on ground infrastructure, the industry is aware that an en-route attack is possible, due to the classified experiment of the Department of Homeland Security on penetrating the aircraft systems remotely. The team, from Robert Hickey's public statements, found vulnerabilities in the radio communication links . Another incident, this time carried out by a citizen, occurred in Germany in 2021, where a man used a simple construction of two radio sets to impersonate an air traffic controller .

In the aviation network, there are a multitude of nodes that are necessary for safety/security and simultaneously inspirational for bad actors. One such node is the ADS-B system, whose technical specifications inherently make it susceptible to jamming and spoofing . All the while, it is a newly implemented system, whose utility in providing more accurate and timely reports on more than aircraft position is recognized and thought to be superior to radar.

5. Flightradar24 -the most popular application

Flightradar24 – a website showing the location of aircraft on the map in real time. The flight path, take-off and landing locations, flight number, aircraft type, position, altitude, flight direction and speed are shown on Google maps . You can also see past flights in fast motion by selecting an airline, aircraft type, region or airport. When you click on an airport, you can see a list of arrivals and departures . The service collects data from many sources, but outside the US it is mostly based on ADS-B (Automatic Dependent Surveilance – Broadcast) receivers operated by volunteers. Airplane icons are from FR24, and photos of specific aircraft are taken from JetPhotos.com based on registration number. On

March 3, 2020, aircraft positions from satellite receivers were added (highlighted in blue), while yellow aircraft icons indicate positions from ground receivers .

Flightradar24 was founded in 2006 as a hobby venture by Swedes of Polish origin Mikael Robertsson and Olov Lindberg , who together with CEO Fredrik Lindahl form the company Svenska Resenätverket AB. The service is available through the website and on mobile devices through applications.

Flightradar24 collects data from several sources:

- Automatic dependent surveillance-broadcast (ADS-B). The primary source is a large number of ADS-B terrestrial receivers that collect data from all aircraft in their area that are equipped with an ADS-B transponder and broadcast this data, usually via ADSL, over the internet in real time. Transponders in aircraft transmit their position (obtained by GPS), registration number, altitude, speed and other flight data. About 65% of aircraft in Europe are equipped with ADS-B, and in the USA about 35%. For example, all Airbus aircraft have ADS-B, but Boeing 707, 717, 727, 737-200, 747-100, 747-200, 747SP do not have it built in, so usually these aircraft are not visible on Flightradar24 unless they have been equipped with ADS-B by operators. Typical ADS-B receivers are SBS-1 by Kinetic Avonics and AirNav by AirNav Systems. Such receivers are owned by volunteer aviation enthusiasts. ADS-B signals can also be received and uploaded to the Internet using programmable radios, e.g. based on the R820T tuner .
- Multilateration (MLAT). The second source is multilateration using Flightradar24 (FR24) receivers. All types of aircraft will be visible in MLAT areas, even without ADS-B, but while 99% of Europe is within range, only a small proportion of the US is equipped with it. At least four MLAT receivers are required to calculate the position of the aircraft.
- North American radar data.
- FLARM: A simplified version of ADS-B with a shorter range (20-100 km), mostly used in smaller aircraft, mainly gliders.
- Satellites equipped with ADS-B receivers receive data beyond the range of ground-based Flightradar24 receivers and transmit the data to the Flightradar24 network.
- Federal Aviation Administration. The deficiencies in the USA are compensated by the data from the Federal Aviation Administration, delayed by 5 minutes, but not all data, e.g. registration, may be provided there.

The website blocks certain ADS-B data from displaying it for "security and privacy" reasons. For example, the position of the aircraft used by the Emperor and Prime Minister of Japan was visible on the site until August 2014, when the Ministry of Defense of Japan requested that the data be blocked . As a consequence, the details of this aircraft are no longer available on the portal. The possibility of attacks on aircraft was discussed.

Flightradar24 gained popularity in 2010 when the media relied on it to cover flight disruptions over the North Atlantic and Europe caused by the eruption of the Eyjafjallajökull volcano.

In 2014 and 2015, many news agencies relied on Flightradar24 data for their coverage of air disasters: the disappearance of Malaysia Airlines Flight 370, the downing of Malaysia Airlines Flight 17 over Ukraine in July 2014, the crash of Indonesia AirAsia Flight 8501 in December 2014, and the crash of Germanwings Flight 9525 in March 2015. Flightradar24 reported that their network traffic then increased 50-fold and caused problems with access to the portal. Many airlines rely on Flightradar24 to locate their aircraft.

The portal partly owes its popularity to the ease of access to information. Almost anyone with a mobile phone and an internet connection can track almost any commercial flight in the world with great accuracy in real time, and check the planes flying over their area, whether they are visible or not. The intent behind Flightradar24 is not malignant but rather for curiosity's sake, with the caveat that it can be taken too far and point to an array of privacy concerns.

The company provides receivers to willing volunteers, especially in areas where there are no receivers yet. By April 2015, it had delivered over 2,000 receivers, and there are approximately 5,000 receivers in its network. Besides a receiver, any aviation enthusiast can assemble the simple construction, made of an SD card, a single-board computer and an ADS-B dongle, to obtain access to a stream of flight data. Furthermore, the enthusiast may compliment their setup with a radio receiver and listen in on air traffic control conversations. It must be emphasized that the observance of aircraft and listening to radio transmissions is not illegal in most countries, with the UK and Germany being exceptions due to exacting communication laws, as long as there is no interference caused by that observer.

6. Conclusion

The aviation industry already holds a status as a safe form of transportation, and technological progress is continually being strived for in order to improve the records further. One such example of drawing a dramatic improvement in aviation operations, is the substitution of radar for Automatic Dependent Surveillance-Broadcast. Aviation regulators in Europe have posited a mandate for ADS-B retrofitting, and the general deadline for all flights under Instrument Flight Rules had passed in 2020. Even though the technology is relatively new, it is starting to become widely accepted worldwide. There are some skeptics, who refer to the hypothetical scenario of stalking, doxing, cyber-attack, unlawful interference, jamming, spoofing, etc. These safety and security concerns are viable because there has been an observable and documented rise in the hacking of aviation actors, especially airlines. Luckily, attacks in the past have affected ground infrastructure, not aircraft during critical stages of flight. The ADS-B could be one source of inspiration for malicious intent because of its vulnerabilities and importance. Therefore, aviation authorities should not be pleased with the success of the ADS-B just yet.

References

[1] J. Black and P. Rogaway. Ciphers with arbitrary finite domains. In B. Preneel, editor, Topics in Cryptology - CT-RSA 2002, volume 2271 of Lecture Notes in Computer Science, pages 185--203. Springer Berlin/Heidelberg, 2002. 10.1007/3-540-45760-7_9.

[2] M. Bellare, T. Ristenpart, P. Rogaway, and T. Stegers. Format-preserving encryption. In M. Jacobson, V. Rijmen, and R. Safavi-Naini, editors, Selected Areas in Cryptography, volume 5867 of Lecture Notes in Computer Science, pages 295--312. Springer Berlin/Heidelberg, 2009. 10.1007/978-3-642-05445-7_19.

[3] M. Bellare, P. Rogaway, and T. Spies. The FFX mode of operation for format-preserving encryption. February 2010.

[4] J. Chen and J. Wu. A survey on cryptography applied to secure mobile ad hoc networks and wireless sensor networks.

[5] P. R. Drouilhet, G. H. Knittel, and V. A. Orlando. Automatic dependent surveillance air navigation system. US Patent 5,570,095, Oct 1996.

[6] Federal Aviation Administration. Air traffic nextgen briefing: Keeping america's skies safe. http://www.faa.gov/air_traffic/briefing/, 2009.

[7] Federal Aviation Administration. FAA's NextGen implementation plan, Mar 2011.

[8] Federal Aviation Administration. FAA aerospace forecast fiscal years 2012--2032.

[9] Funkwerk Avionics, Waal, Germany. RTH60 ADS-B/Mode S Receiver Operation and Installation, document no: 03.231.010.71e/revision 2.05 edition.

[10] J. R. Jochum. Encrypted mode select ADS-B for tactical military situational awareness. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA, Apr 2002.

[11] T. D. Judd. Automatic dependent surveillane data transfer. In AIAA/IEEE Digital Avionics Systems Conference, 8th, volume 2: pages 858--864, San Jose, CA, Oct 1988.

[12] E. Lester and R. J. Hansman. Benefits and incentives for ADS-B equipage in the national airspace system. 2007.

[13] D. Magazu, R. Mills, J. Butts, and D. Robinson. Exploiting the automatic dependent surveillance-broadcast system via false target injection. to appear in Journal of Aviation and Aerospace Perspectives.

[14] D. McCallie, J. Butts, and R. Mills. Security analysis of the ads-b implementation in the next generation air transportation system. International Journal of Critical Infrastructure Protection, 4(2):78--87, 2011.

[15] T. McParland, V. Patel, and W. Hughes. Securing air-ground communications. In Digital Avionics Systems, 2001. DASC. 20th Conference, volume 2, pages 7A7/1--7A7/9 vol.2, Oct 2001.

[16] K. Sampigethaya and R. Poovendran. Privacy of future air traffic management broadcasts. In Digital Avionics Systems Conference, 2009. DASC '09. IEEE/AIAA 28th, pages 6.A.1-1--6.A.1-11, oct. 2009.