EUROCONTROL

Air Traffic Management
A Cybersecurity Challenge

SUPPORTING EUROPEAN AVIATION

FOUNDING MEMBER
SESAR
JOINT UNDERTAKING

NETWORK
MANAGER

John Hird is a member of the Air Traffic Management Security Unit in the EUROCONTROL Civil Military Cooperation Division.

The Unit's work programme focusses on enhancing levels of Air Traffic Management security through international collaboration and implementation support to Member States and stakeholders.

Contact: *atmsecurityunit@eurocontrol.int*

EUROCONTROL
DECMA/CMC
96, Rue de la Fusée
1130 Belgium

Supporting every aircraft in flight is an unseen, complex, global infrastructure called the Air Traffic Management (ATM) system, which ensures that safety and security are routinely maintained. As the digitalisation of aviation proceeds at pace, ATM is evolving in parallel to deliver new services seamlessly and cost-efficiently. This report reveals how the system is changing, and how regulators and other ATM stakeholders are working together to ensure that cyber-resilience is maintained.

Aerodromes are familiar places for the flying public, but few are aware of the Air Traffic Management (ATM) system that supports aircraft in transiting from departure to destination. The ATM system comprises a variety of physical, organisational, information and human assets, interacting in a complex system of systems to deliver a seamless travelling experience to passengers. Operational stakeholders include Air Navigation Service Providers (ANSPs) and the EUROCONTROL Network Manager (NM), working together to deliver air traffic flow and capacity management (ATFCM). The goals of ATM are to expedite flights safely, balancing capacity and demand by providing effective flow management to minimise delays, and to do so cost-effectively while limiting environmental impacts.

However, the current system used to do this is a patchwork of evolving, interconnected systems, comprising bespoke legacy systems and more recent commercial off-the-shelf (COTS) systems, connected by a variety of interfaces utilising a combination of national, international and proprietary standards. These include ground and space-based communication, navigation, and surveillance (CNS) systems, air traffic control centres (ATCs), airports, control towers, and the information used by and exchanged between systems as aircraft are assisted through controlled airspace. The diversity of systems has, as we will see, significant implications for cybersecurity.

> *"…the system had to be shut down when its integrity was compromised by a viral attack…"*

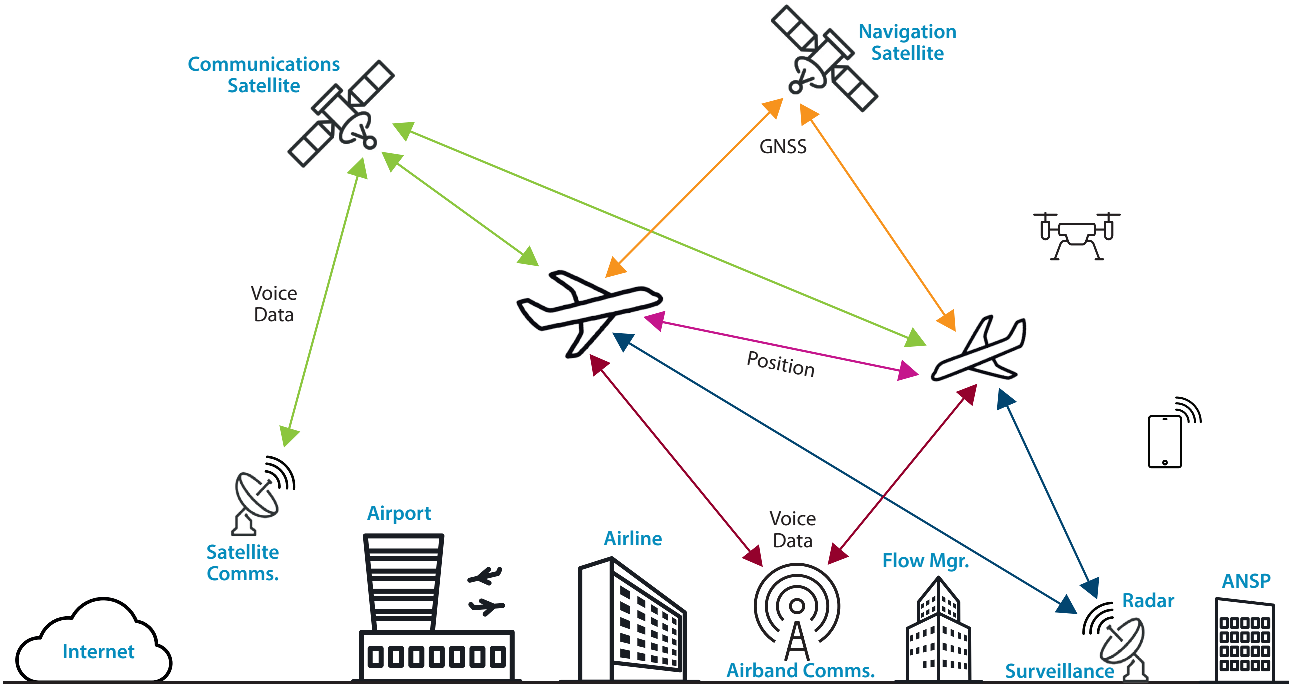

Figure 1 - Complex System of Systems

Digitalisation

The digitalisation of aviation is proceeding at pace, and the architecture of the future European ATM system will rely on increased interconnectivity, based on modern technologies and enhanced interoperability, to deliver new operational concepts building on the sharing of information. The following are examples of where digitalisation is impacting aviation.

System Wide Information Management (SWIM) is a new concept for the efficient exchange of information between aviation stakeholders, comprising aeronautical, flight, meteorological, air traffic flow, and surveillance information. SWIM aims to replace the current plethora of separate systems and connections by one SWIM system which provides a set of services to stakeholders based on standard specifications, a single governance framework, and a common set of infrastructure components.

From an information viewpoint, SWIM will provide interoperable services using seamless data exchange between data providers and data users, by applying open standards on an IP-based[1] network. The availability of SWIM will facilitate the development and deployment of several new concepts in aviation, including the concepts of the Remotely Operated Tower and Virtual Centre.

The use of Global Navigation Satellite Systems (GNSS - e.g. GPS, Galileo, GLONASS) is standard practice in aviation, and augmentation systems have been developed to monitor and improve the performance of GNSS in terms of accuracy, integrity, continuity, and availability. For example, the European Geostationary Navigation Overlay Service (EGNOS) [1] is a regional Satellite-Based Augmentation Service (SBAS) which complements the existing GNSS services. Here, differential corrections and integrity messages are broadcast over vast areas by geostationary satellites as an augmentation, or overlay, of the original GNSS messages, and are accessible to all with the appropriate equipment. EGNOS provides a wide area augmentation service over Europe, whilst WAAS[2] [2] and MSAS[3] [3] provide similar services over the USA and Japan respectively. OMNISTAR and StarFire are global SBAS systems. The Ground-Based Augmentation System (GBAS), specific to civil-aviation, is a safety-critical system which supports local augmentation of the primary GNSS constellation, providing enhanced levels of service to support precision services such as approach and landing operations at airports. The main goal of GBAS is to provide integrity assurance, but it also enhances accuracy. In common with other wireless protocols in aviation however, GNSS systems possess known vulnerabilities [4].

[1] *IP – Internet Protocol*

[2] *WAAS – Wide Area Augmentation System*

[3] *MSAS - MTSAT Satellite Augmentation System (MTSAT – Multifunctional Transport Satellites)*

The aviation ecosystem is being further diversified by the rapid addition of unmanned aerial vehicles, such as RPAS[4]. An RPAS consists of an airborne platform and a remote pilot station, supported by a traffic management ecosystem for uncontrolled operations (UTM[5]) that is separate from, but complementary to, the ATM system, and presents a number of particular cybersecurity challenges. The reliance on wireless communications for command and control makes them vulnerable to a variety of attacks, with potential consequences which include the following: loss of control; hi-jacking of the aircraft; theft of the aircraft and payload; use as a platform for jamming, spoofing or eavesdropping; use as a weapon.

The concept of urban air mobility (UAM[6]) leverages the sky to move passengers sustainably, and contribute positively to improved links between cities and regions using a multimodal transport system. The establishment of UAM is expected to result in a further significant increase in air vehicles, including *flying taxis*.

Virtual centres [5] are another example of digitalisation, allowing more flexible and efficient ways of working, and facilitating collaboration between ANSPs. In a virtual centre, ATM data services (such as flight data, radar, and weather information) can be geographically decoupled from physical controller working positions, delivering increased agility and capacity, while enabling better contingency planning. This could deliver greater flexibility in organising ATM operations and, in doing so, provide seamless and more cost-efficient service provision to airspace users.

In connected aircraft, digital services support the use of Electronic Flight Bags (EFB) by pilots, hand-held devices by passengers and crew, infotainment systems, and real-time aircraft engine monitoring. The Internet of Things (IoT) facilitates passenger flow management and baggage tracking in airports [6]. For such new concepts to be successfully deployed operationally, they must be resilient to current and emerging security threats.

In Europe, the Flightpath 2050 document of 2011 [7] envisaged the evolution of a multi-mode, integrated transport system, which would enhance data sharing between transport modes to optimise travel times, enhance the passenger experience, and optimize the transit of goods.

[4] *RPAS - Remotely Piloted Aircraft Systems*
[5] *UTM – Unmanned aircraft system Traffic Management*
[6] *UAM – Urban Air Mobility*

This emerging integration of multiple transport services into a single mobility service is termed Mobility as a Service (MaaS). A MaaS provider would be able to offer a diverse menu of transport options drawn from various transport modes, and add value to users by providing the best value proposition, via a single application, and a single payment channel. At the moment, road, rail, water and air transport modes have different security postures and needs, while realising the potential benefits of MaaS requires secure information sharing between modes and the harmonisation of security levels across them.

Some issues that may elevate risk in future ATM systems include the following:

- Increased interconnectivity and integration between different civil and military actors (ANSPs, airlines, airports, aircraft) and CNS systems;
- Greater use of COTS products and open protocols for networking and communications;
- An attack on one system could propagate to impact a large geographical area;
- Certain legacy wireless protocols in aviation possess known vulnerabilities;
- The interconnection of legacy systems to modern networks may create vulnerabilities;
- The introduction of new vehicles, such as drones, into controlled airspace adds another dimension of complexity and risk;

- The development of Mobility as a Service (MaaS) in Europe will require secure information-sharing between transport modes.

The rapid pace of digitalisation in the evolving system has resulted in cybersecurity becoming increasingly important to ATM stakeholders. Thanks to its strong focus on safety, ATM already benefits from extensive redundancy (the duplication of critical components to provide fail-safes if primary mechanisms malfunction), and the existence of fall-back systems and procedures supporting non-nominal operations, meaning that the system is fundamentally robust. However, ATM is transitioning into an increasingly new environment, where the application of new approaches to system development and operation is a prerequisite to limit the effects of unlawful interference by intelligent adversaries.

Potential Impact of a Security Breach

There are several potential consequences of a security breach. Service provision could be disrupted, causing congestion, delays or service termination. An insecure system may have an impact on safety. In certain scenarios, the impact on passengers or personnel could include stress, injury, or in the worst case, fatalities. An incident could also result in financial losses, or in severe cases, bankruptcy. Reputational issues resulting from negative publicity around a breach could affect future business opportunities. The ease with which information in certain wireless protocols used for CNS (e.g. ACARS[7], AeroMACS[8], ADS-B[9]) can be eavesdropped upon and used for criminal purposes has triggered both privacy issues and data confidentiality concerns.

[7] *ACARS – Aircraft Communications Addressing and Reporting System*

[8] *AeroMACS – Aeronautical Mobile Airport Communications System datalink*

[9] *ADS-B – Automated Dependent Surveillance - Broadcast*

ATM Cyber-attacks and Incidents

Cyber-attacks in aviation are not new. In 1997 the breach of a Bell Atlantic control system used for air traffic communications at Worcester airport in Massachusetts (USA) [8], caused a system crash that disabled the phone system at the airport for six hours, halting telephone services to the control tower, airport security, the airport fire service, the weather service, and aircraft operators. The attack also took out the tower's main radio transmitter, a transmitter for controlling runway lights, and a printer used by controllers to monitor flight progress. Telephone services to 600 homes in the vicinity were also halted.

One of the first widely documented incidents in ATC occurred in an FAA system in Alaska in 2006 [9]. The system had to be shut down when its integrity was compromised by a viral attack which spread from administrative networks, highlighting the importance of isolating operational systems. In 2008, hackers breached the integrity of the FAA system over a wide area.

The manipulation of satellite navigation signals has become mainstream, with several incidents documented in Russian waters since 2017 [10]. These attacks resulted in ships' navigation systems indicating the vessels to be in different locations than in reality. Although targeted at shipping, such attacks would impact other GNSS users in the region.

In 2018, a third party conducting mandatory background checking of airport workers for the Australian Government was hacked [11], resulting in the exposure of personal details of hundreds of aviation employees, causing concern in terms of the invasion of privacy for workers, the potential malicious use of the information by criminals, and the vulnerability of the aviation system.

In 2020, British Airways (BA) was fined £20m [12] for failing to protect the personal and financial details of more than 400,000 of its customers, which were accessed via a cyberattack resulting from a failure to adequately secure its business systems. The fine was imposed as a result of breaching the General Data Protection Regulation (GDPR) [13], a European Union law which requires organizations to safeguard personal data and uphold the privacy rights of anyone in EU territory. A GDPR Enforcement Tracker website [14] provides an overview of fines and penalties which data protection authorities within the EU have imposed. Not all fines are made public.

The advent of affordable software-defined radios (SDRs), has made the reception of ADS-B messages and the positional tracking of many aircraft trivial. A personal SDR receiver can provide a range of up to 600 km radius, while commercial and non-profit organisations such as *Flightradar24*, *PlaneFinder*, *FlightAware*, *ADSBexchange*, *Radarbox25*, and *OpenSky*, pool the data and make it available online, adding a global dimension to the tracking of aircraft. The data on these services is largely publicly available and easily accessible. However, it may exclude aircraft considered sensitive, such as those owned by governments or corporations. Unfiltered ADS-B data,

easily obtained from several sources, can impact the privacy of aviation users when used in conjunction with publicly available aircraft meta-data. There are several documented examples demonstrating the ease with which this information can be accessed and analysed to expose confidential information. For example, investigative journalists used such data to expose CIA rendition flights which occurred during the 'war on terror' [15]. Similarly, such data has been used to reveal meetings between business executives, providing clues on future mergers and acquisitions [16], and to infer meetings between governments. Consequently, exploitation of such data can potentially be used to infer confidential information in a number of areas, including national security, diplomacy, and business competitiveness. Protecting the privacy of non-commercial aviation users in the future may require further regulatory and technical developments to be made.

Information from EUROCONTROL's European ATM Computer Emergency Response Team (EATM-CERT) provides an insight into a wide spectrum of security incidents reported by aviation stakeholders in 2019, of which 20% targeted ANSPs. In terms of event severity, 80% were classified as low, 20% were medium and, fortunately, none were high. The consequences of the attacks were primarily the leaking of sensitive documents (47%) and data theft (35%), including network schematics and user credentials for sensitive systems. Threat actors were generally cyber-criminals and state-sponsored groups, with the main motives being to target airspace users for financial gain, and/or acquire the intellectual property of equipment manufacturers.

"…the manipulation of satellite navigation signals has become mainstream…"

The report emphasises the importance of a holistic approach to security, suggesting that excessively focusing on technical controls at the expense of people and processes may expose exploitable vulnerabilities. As security expert Bruce Schneier underlines, "*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology*". The report also highlights the importance of securely sharing anonymised security incident information, since this allows others to improve their security posture.

Attackers are resourceful and adapt to changing circumstances. The year 2020 has seen criminal groups deploying COVID-19 themed lures for phishing purposes. There is also evidence that remote working, which has massively increased for many white-collar workers during the pandemic, significantly increases the risk of a successful attack, due to weaker controls being present in home IT networks and systems.

Responding to the Challenge

In recognition of the challenge of developing cyber-secure and resilient ATM systems, recent amendments to the International Civil Aviation Organisation (ICAO) Annex 17 Standards and Recommended Practices (SARPs) [17] and associated guidelines explicitly address cybersecurity.

In Europe, in order to promote a harmonised approach to meeting Annex 17 SARPs, the current ATM-specific Implementing Rule is IR (EU) 2017/373 [18] which, coupled with amendment 2020/469 [19], specifies security requirements for ANSPs, the EUROCONTROL NM, and ATFCMs. This regulation compels operators to adopt a broad-based, holistic approach to security, addressing people, processes, and technology, beginning with the requirement to implement a Security Management System (SeMS) to protect facilities, personnel, service provision, and operational data.

In order to bolster their defences and protect their systems from attack, operators must perform security risk assessments, implement security controls to mitigate identified risks, and perform security monitoring and improvement activities. Where appropriate, personnel must also be security-cleared. When their defences are compromised, operators must detect these breaches, alert personnel, contain the effects of the breaches, and identify recovery and mitigation actions based on contingency plans.

The regulation of unmanned aircraft was initially addressed by the updated EASA basic regulation (IR (EU) 2018/1139) [20], which applied to both manned and unmanned aircraft. To further support the safe and secure operations of unmanned aircraft, two specific regulations were introduced ([21], [22]) which included requirements on cybersecurity.

The challenge of making systems cyber-resilient is exacerbated by the increasing importance of artificial intelligence (AI), which is set to have a profound influence on aviation in the future. The *Fly AI Report* [23] developed by the European Aviation AI High Level Group provides a comprehensive overview of current and expected uses of AI in aviation, including an analysis of how AI may support aviation cyber-resilience. EASA's AI roadmap [24] discusses the implications of AI on aviation and the challenges which it brings to the sector, and addresses the notion of the trustworthiness of AI. Developments in machine- and deep-learning will increase the resilience of systems and services in, for example, malware detection, network analysis, message filtering, and providing support to human operators [25]. However, AI can also be used to attack systems [26], and will change the nature of the attack surface accessible to malicious actors. In the security operations centre of the future, AI may contribute to the automation of cyber-defences in areas such as vulnerability identification, predicting the evolution of threats, and adaptively mitigating attacks in real-time.

European Regulatory Complexity

In addition to complying with aviation-specific European regulations, operators may also have to comply with other legal instruments that apply to industry in general, such as GDPR [13], the Network and Information Security (NIS) Directive [27], and the Cybersecurity Act [28], which can make the task of maintaining regulatory compliance rather complex. If an operator happens to be designated as part of 'critical infrastructure' or as a 'provider of an essential service', it may also become subject to additional regulations and be required to report to additional authorities.

"...operators must perform security risk assessments, implement security controls to mitigate identified risks, and perform security monitoring and improvement activities..."

For example, the EU Common Requirements Regulation [18] lays down security requirements to be followed by ANSPs, with audits being carried out by the National Supervisory Authority (NSA) or the European Union Aviation Safety Agency (EASA). However, if an ANSP is also designated as a provider of an essential service, it must comply with the NIS Directive, and coordinate with the National Competent Authority (NCA) and/or the Computer Security Incident Response Team (CSIRT) for the notification of incidents having a significant impact on service provision. It must also comply with the Cybersecurity Act, so its products, services, and processes are subject to the European Cybersecurity certification framework via ENISA.

This results in a more complex governance framework for essential service providers, requiring the creation of additional roles and bodies, and resulting in additional coordination both within and outside member states. This situation is replicated in all transport modes.

To address this complexity, rationalisation and harmonisation of the regulatory framework is currently being tackled by the European Union Aviation Safety Agency (EASA) and a number of aviation stakeholders in the European Strategic Coordination Platform (ESCP), which promotes international cooperation and harmonisation in risk management, risk information-sharing between organisations, and risk assessment methods. To this end, the ESCP has developed a Strategy for Cybersecurity in Aviation [29] to make aviation an evolutionary cyber-resilient system, adopting a 'built-in' security approach and addressing security from a system's conception through its development, deployment, and operations. Comprehensive guidance material and acceptable means of compliance for the security certification of ATM systems will soon be provided to operators. More recently, the European Commission has established the EU Aviation Cybersecurity Working Group. The objective of this group is to better align the regulatory frameworks on cybersecurity in the aviation sector.

Conclusion

As we have seen, there are many potential impacts of security incidents in ATM, some of which have consequences for broader society and have an impact on third parties outside of the aviation system. With the ongoing digitalisation of ATM, a system-wide, holistic approach to cybersecurity is required to ensure that ATM remains cyber-resilient.

To permit the safe and secure incorporation of new vehicles in the air, UTM services must also be cyber-resilient, as must be the interface to ATM and to the services provided by an integrated UTM and ATM system. These are pre-requisites for the future safe and secure deployment of new vehicles and the provision of novel services such as drone deliveries and UAM.

The emergence of multi-mode transport services supporting MaaS will be facilitated by harmonising security levels across transport modes, and by enabling secure data sharing between them to maintain transport system resilience and ensure the personal privacy of passengers and the security of their personal data.

In order to address the threat posed by adversaries seeking to exploit the weakest link in the aviation system, information sharing on security incidents is becoming increasingly important to stakeholders, and will be of mutual benefit in improving their security postures.

As the pace of innovation in aviation accelerates, a multitude of actors in aviation are seeking to harmonise the regulatory framework and develop the methods, tools, standards and guidance material needed to ensure that cyber-resilience is maintained and improved in the current system. Steps are also being taken to improve in these areas and to develop in the areas of security certification and oversight in order to meet the challenges of the future. EUROCONTROL will continue to support its aviation stakeholders in meeting these challenges.

EUROCONTROL and ATM Cybersecurity

EUROCONTROL is involved in ATM cybersecurity at several levels. At ICAO, it contributes to the Aviation Security (AVSEC) Threat and Risk Working Group (TRWG) and the Secretariat Study Group on Cybersecurity (SSGC), and is an observer on the AVSEC Panel.

In Europe, it participates in the Stakeholders Advisory Group on Aviation Security (SAGAS) at the European Commission (EC), and participates in EASA's ESCP. It also participates in the European Civil Aviation Conference's (ECAC) Security Forum, the Guidance Material Task Force (GMTF), and the study group on cyber threats to aviation. EUROCONTROL also takes part in European Organisation for Civil Aviation Equipment (EUROCAE) working groups, including WG-72 (Aeronautical Systems Security), developing security certification standards for both ground and airborne systems. It led the development of ED205, which delivered a process to assess the security of ATM/ANS ground systems, and leads the development of its successor, ED205A, in cooperation with Special Committee 216 of the RTCA[10] to ensure compatibility with the associated US standard.

Along with the EC, EUROCONTROL is a co-founder of the Single European Sky ATM Research (SESAR) programmes, participating in the development of security risk assessment methods, tools, and guidance material for the SESAR and SESAR2020 programmes [30], which aim at developing new concepts and technologies in aviation. In the meantime, planning for the future SESAR3 programme is in progress. EUROCONTROL also participates in the Advisory Council for Aeronautics Research in Europe (ACARE) and has the role of security co-chair in the Safety and Security Working Group (WG4).

EUROCONTOL is the home of the EATM CERT[11], which supports EUROCONTROL services and products and ATM stakeholders in protecting themselves against cyber threats that could impact operational IT assets and data. To provide these services, the organisation collaborates with national and international ATM stakeholders, ATM manufacturers, sectoral and national CERTs, EASA, the European Centre for Cyber Security in Aviation (ECCSA), information sharing and analysis centres (ISACs), Europol and others. It is also involved in cybersecurity awareness building and training, delivering courses at EUROCONTROL's training centre in Luxembourg[12], and providing tailored cybersecurity workshops to ANSPs, civil aviation authorities, and national supervisory authorities in member states.

[10] *RTCA – Radio Technical Commission for Aeronautics*

[11] *https://www.eurocontrol.int/service/european-air-traffic-management-computer-emergency-response-team*

[12] *https://trainingzone.eurocontrol.int*

References

[1] *What is EGNOS?*, European Space Agency.
Available at http://www.esa.int/Our_Activities/Navigation/EGNOS/What_is_EGNOS

[2] *Satellite Navigation – Wide Area Augmentation System*, Federal Aviation Administration (FAA). Available at https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/waas/

[3] *MSAS General Introduction*, European Space Agency.
Available at https://gssc.esa.int/navipedia/index.php/MSAS_General_Introduction

[4] Strohmeier M., *Security in Next Generation Air Traffic Communication Networks*, PhD Thesis, University of Oxford, Trinity College, 2016.

[5] *Taking Virtual Centres to the Next Level*, October 2019, SESAR Joint Undertaking.
Available at https://www.sesarju.eu/news/taking-virtual-centres-next-level

[6] Drinkwater D., *Ten stellar real-life examples of IoT taking flight in aviation*, Internet of Business, August 2016.
Available at https://internetofbusiness.com/10-real-life-examples-iot-aviation/

[7] *Flightpath 2050 – Europe's Vision for Aviation – Report of the High Level Group on Aviation Research*, European Commission, 2011.

[8] Rindskopf A., *Juvenile Computer Hacker Cuts Off FAA Tower*, Press Release, Irational.org, March 1998.
Available at http://www.irational.org/APD/CCIPS/juvenilepld.htm

[9] *Review Of Web Applications Security And Intrusion Detection In Air Traffic Control Systems*, Federal Aviation Administration, Report Number: FI-2009-049, May 4, 2009.

[10] Goward D., "*Mass GPS Spoofing Attack in Black Sea?*", The Maritime Executive, 11.07.2017.
Available at https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea

[11] Pash C., *Cyber security is being tightened at Australian airports after an identity card data hack*, July 2018, Business Insider Australia.
Available at https://www.businessinsider.com.au/identity-card-data-hack-data-breach-australian-airports-2018-7

[12] *ICO fines British Airways £20m for data breach affecting more than 400,000 customers*, October 2020, Information Commissioner's Office. Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on *the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).*

[14] *GDPR Enforcement Tracker*. Available at https://www.enforcementtracker.com/

[15] *The Rendition Project*. Available at https://www.therenditionproject.org.uk/index.html

[16] Martin Strohmeier, Matthew Smith, Vincent Lenders, Ivan Martinovic,*The Real First Class? Inferring Confidential Corporate Mergers and Government Relations from Air Traffic Communication, 2018 IEEE European Symposium on Security and Privacy (EuroS&P)*, London, 2018.

[17] ICAO Annex 17 to the Convention on International Civil Aviation, *Safeguarding International Civil Aviation Against Acts of Unlawful Interference.*

[18] Commission Implementing Regulation (EU) 2017/373, *laying down common requirements for providers of air traffic management / air navigation services and other air traffic management network functions and their oversight...*, 17th October 2011

[19] Commission Implementing Regulation (EU) 2020/469, *amending … as regards requirements for ATM/ANS, design of airspace structures and data quality, …,* 14th February 2020.

[20] Regulation (EU) 2018/1139, on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency …, 4th July 2018.

[21] Commission Delegated Regulation (EU) 2019/945, *on unmanned aircraft systems and on third-country operators of unmanned aircraft systems*, 12th March 2019.

[22] Commission Implementing Regulation (EU) 2019/947, *on the rules and procedures for the operation of unmanned aircraft*, 24th May 2019.

[23] *The Fly AI Report – Demistifying and Accelerating AI in Aviation/ATM,* March 2020, European Aviation Artificial Intelligence High Level Group.

[24] *Artificial Intelligence Roadmap – A human-centric approach to AI in aviation*, Version 1.0, EASA, February 2020.

[25] *Artificial Intelligence - A European Perspective*, European Commission, Joint Research Centre, 2018.

[26] Brundage, et al, *The Malicious Use of Artificial Intelligence: Forecasting*, Prevention, and Mitigation, Future of Humanity Institute, University of Oxford, February 2018.

[27] Directive (EU) 2016/1148, *concerning measures for a high common level of security of network and information systems across the union*, 6th July 2016.

[28] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on *ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).*

[29] *Strategy for Cybersecurity in Aviation*, EASA European Strategic Coordination Platform, September 10th, 2019.

[30] *A proposal for the future architecture of the European airspace*, SESAR Joint Undertaking, 2019.
Available at https://www.sesarju.eu/node/3253

EUROCONTROL

SUPPORTING EUROPEAN AVIATION

www.eurocontrol.int