Journal of İstanbul School of Technology - JISTECH

Volume 1, Issue 2 – December 2025, ISSN: 3108-4427

Policy for Building Resilience to Cyber Threats in Civil Aviation

Grzegorz K. ZAJAC[a]

a: Ph.D., University College of Professional Education in Wroclaw, Poland, 0000-0002-5504-5228, gkzajac@wp.pl

Submitted: 10.10.2025, Accepted: 14.11.2025, Published: 08.12.2025

Cite APA: Zajac, G.K., (2025). Policy for Building Resilience to Cyber Threats in Civil Aviation, Journal of İstanbul School of Technology (JISTECH), 1(2), pp. 350-371. , DOI:…

ABSTRACT

Building resilience to cyber threats requires the synergy of regulatory, operational, and educational actions in order to effectively protect the aviation sector. The aim of the article will be an analysis of dynamically developing digital threats in the aviation industry and the ways of counteracting them. An identification of threats in civil aviation will be carried out. Due to the fact that, along with the progressing digitalization of aviation infrastructure and operations, the risk of cyberattacks is increasing, which may disrupt the functioning of navigation systems, reservation systems, or airport infrastructure. The main international and European regulations and the strategies for counteracting these threats will be discussed, both by intergovernmental organizations such as ICAO, the EU, or EASA, but also by industry non-governmental organizations such as IATA. Key challenges and the necessity of developing a culture of digital security will also be analyzed.

Keywords: *cyberattacks, civil aviation, cybersecurity, cyber threats*

1. RESEARCH SUBJECT AND METHODOLOGY

In the era of digitalization and the growing dependence of aviation on advanced technologies, cybersecurity is becoming one of the most important challenges for this sector. Civil aviation is an industry that can be described as "vulnerable" in relation to threats associated with cyberspace and cyberattacks. An extremely important role in this context is played by the state through performing and exercising the regulatory, supervisory, coordinating, and operational functions. An important objective is to build resilience to cyber threats through the development of appropriate regulations, strategies, and technologies, as well as strengthening international cooperation and the exchange of information. This study will discuss the main challenges in this area, the applicable legal regulations, and the practical actions undertaken by the aviation sector in order to increase resilience to cyber threats.

The main aim of the article is to analyze the dynamically developing digital threats in the aviation industry and the ways of counteracting them. The study conducted an analysis of digital threats in civil aviation resulting from the growing dependence on advanced technologies, which increases the risk of cyberattacks disrupting the functioning of critical systems. The subject of the research is resilience to cyber threats in civil aviation, including contemporary challenges, regulations, and strategies for counteracting them. The analysis will cover the main international and European regulations, the strategies for counteracting threats implemented by organizations such as the International Civil Aviation Organization (ICAO) and the European Union (EU), as well as the role of the state and the necessity of developing a culture of digital security.

This study has an analytical and descriptive character. In order to achieve the adopted research objective, methods characteristic of social sciences and legal sciences were used. The study primarily applied the method of literature and document review, which made it possible to conduct an overview and analysis of scientific publications and normative documents in the field of cybersecurity and civil aviation. The legal-dogmatic method was also used, which was necessary for the detailed interpretation and analysis of

applicable legal regulations, both at the international level (ICAO) and at the European level (the NIS 2 Directive, the guidelines of the European Union Aviation Safety Agency – EASA), in order to determine their content, meaning, and mutual relations. In addition, the method of literature criticism was applied in order to obtain an in-depth understanding and assessment of the positions of experts and international organizations in relation to contemporary challenges and the necessity to develop a culture of digital security in the aviation sector. The research material included legal acts, guidelines, recommendations, and scientific publications concerning the identification of threats and the building of resilience to cyberattacks in the aviation environment.

The research problem of the article can be formulated as a main question that the article aims to answer: in what way do international and European regulations and strategies contribute to building the resilience of civil aviation to dynamically developing cyber threats, and what are the main challenges in effectively implementing these mechanisms. The hypothesis assumes that building effective resilience of civil aviation to dynamically developing cyber threats is possible through the comprehensive integration of global standards established by ICAO with the regional regulations of the European Union, as well as through the synergistic use of the functions of the state, which constitutes a necessary condition for ensuring the protection of critical operational systems and minimizing the risk of cyberattacks.

2. RESEARCH RESULTS

Increasing interdependencies mean that disruptions in one sector can immediately affect the functioning of other sectors: an attack on electricity producers may, for example, paralyze airports. A similar situation occurs with unmanned aircraft (drones). Public spaces are particularly vulnerable to attacks carried out with drones. The attacks may be directed at individuals, gatherings, critical infrastructure, state institutions, state borders, or public spaces. Such a situation highlights the urgent need to implement modern and technologically advanced protection systems.

Cyber threats, both those resulting from external attacks and internal irregularities, may lead to disruptions in the functioning of critical operational systems, such as air traffic control systems or ground traffic management. In this regard, it is necessary to continuously invest in modern security technologies, staff training, and the development of incident response procedures in order to minimize the risk of escalation of the effects of cyberattacks and to protect the integrity of the entire air transport system.

It should be noted that there is a need for the continuous updating of international and national regulations in the area of cybersecurity in civil aviation, while ensuring joint action by all relevant stakeholders. Resilience to cyber threats in this field requires comprehensive cooperation between the state, the aviation industry, international organizations, and cybersecurity experts. Information exchange, the standardization of procedures, and continuous investment in the development of modern technologies appear to be extremely important, as they jointly enable the construction of coherent and effective defense systems. It is worth noting that the guidelines of ICAO and EASA, as well as the recommendations of IATA, establish security frameworks, enabling the implementation of uniform standards and procedures aimed at minimizing the risk of cyberattacks.

Development of technology in aviation increases the attack surface and forces the use of proactive defense strategies. Ukwandu et al. (2022) emphasize that the growing dependence on information systems, which enable the maintenance of high-quality services, significantly increases the risk of cyberattacks. They point out that numerous entry and exit points in integrated aviation systems generate new security gaps, and problems related to outdated IT infrastructure and system fragmentation further deepen the challenges faced by the aviation sector (Ukwandu. 2022. 146).

Cyberthreats, both those resulting from external attacks and those arising from internal irregularities, can lead to disruptions in the functioning of critical operational systems, such as air traffic control systems or ground traffic management. Consequently, it is necessary to continuously invest in modern security technologies, personnel training, and

the development of incident response procedures in order to minimize the risk of escalation of cyberattack effects and to protect the integrity of the entire air transport system.

The research results confirm that civil aviation is a sector exceptionally vulnerable to cyber threats and requires comprehensive cooperation between the state, individual aviation entities, and international organizations. In the conclusion, it will be indicated that building resilience requires the synergy of regulatory, operational, and educational actions, and that European and international standards constitute the legal foundation for aviation entities in the area of cyber risk management.

3. THE ROLE OF ICAO IN SHAPING GLOBAL CYBERSECURITY STANDARDS IN CIVIL AVIATION

Discussions by the International Civil Aviation Organization (ICAO) on cybersecurity began at the beginning of the 21st century, when the growing dependence of civil aviation systems on digital technologies was observed. Initially, these issues were marginal and were limited to the protection of communication and navigation systems. Over time, however — along with the development of the concept of digital aviation — ICAO's activities came to cover the entirety of aviation infrastructure, from air traffic management to information security at airports and in onboard aircraft systems..

The Organization has developed a number of normative and strategic documents that have become the foundation of the global approach to cybersecurity in aviation. These include:

a) Annex 17 to the Chicago Convention (Annex 17 — Security: Safeguarding International Civil Aviation against Acts of Unlawful Interference),
b) Doc 9985 — Cybersecurity Manual,
c) Cybersecurity Strategy in Civil Aviation,
d) Cybersecurity Action Plan.

Annex 17 currently contains provisions obligating the Member States to protect information and communication systems against unauthorized access, manipulation, and

cyberattacks. In turn, the Cybersecurity Manual (Doc 9985) has an operational character and includes detailed guidelines concerning risk management, incident response, and the integration of physical and digital security aspects in the ATM environment. This document, although formally restricted, is widely recognized as the fundamental tool for the implementation of ICAO principles by States and by entities within the aviation sector.

In light of these documents, ICAO Member States are obliged to ensure the protection of aviation systems against cyberattacks and to develop mechanisms for international cooperation in the exchange of information on threats, system vulnerabilities, and best practices. ICAO has thus created a framework that enables States to build coherent national policies based on common standards and mechanisms for data exchange.

An important element of the Organization's activities are the decisions taken during the sessions of the ICAO Assembly. During the 41st Session of the Assembly, held from 27 September to 7 October 2022, states were once again urged to ratify the 2010 Beijing Convention (Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation) and the 2010 Beijing Protocol, which expand the catalogue of acts of unlawful interference to include actions committed by means of information technologies. In this way, ICAO recognized a cyberattack as a potential offence against the safety of civil aviation.

In 2019, during the 40th Session of the Assembly, the *Aviation Cybersecurity Strategy* was adopted, followed by the *Cybersecurity Action Plan*, which defined specific actions for States, aviation entities, and international organizations. These documents set the directions for developing a cybersecurity culture in aviation and for building a global system for sharing information on threats and incidents. As part of the implementation of the strategy, ICAO developed a number of tools supporting Member States and aviation entities, including:

a) Cybersecurity Culture in Civil Aviation (ICAO, 2022) — a document promoting the development of a cybersecurity culture among the personnel of aviation entities and strengthening the organizational resilience of the sector,
b) Cybersecurity Policy Guidance (ICAO, 2022) — a guide supporting States and the aviation industry in creating a systemic approach to cybersecurity management, covering both modern and legacy information systems. It also indicates ways of responding to incidents and restoring operational capability while minimizing disruptions to air traffic,
c) Cyber Information Sharing (ICAO, 2024) — the latest guidelines concerning the sharing of information on cyber threats, covering the principles of classifying information, verifying its reliability, and organizing national and regional data-sharing systems.

Additionally, the ATM Security Manual (Doc 10088) emphasizes the necessity of a holistic approach to security, combining elements of physical, organizational, and digital protection within air traffic management systems. All these initiatives confirm that ICAO does not limit itself solely to establishing regulations, but actively supports states and other aviation entities in building a global culture of digital resilience.

The significance of these activities is fundamental: they establish global cybersecurity standards in aviation, enabling international coordination and cooperation, and supporting the prevention of cross-border cyberattacks. In practice, ICAO serves as the main platform for international dialogue in the field of protecting the digital aviation infrastructure, and its documents constitute a point of reference for the harmonization of national regulations with global safety standards.

4. STRATEGIES AND CHALLENGES IN BUILDING RESILIENCE TO CYBER THREATS

Modern civil aviation has become one of the most technologically advanced and at the same time one of the most exposed sectors of critical infrastructure. The progressing

digitalization of air traffic management processes, airport operations, communication and navigation, as well as the integration of information systems within the European ATM network, have caused cyber threats to become a real risk to the operational safety and security of air transport.

In recent years, the European Union has undertaken a number of actions aimed at strengthening the resilience of Member States to contemporary threats, including those of a digital nature. A key role is played by two complementary initiatives announced by the European Commission in 2020:

a) European Union Security Union Strategy 2020–2025 (European Commission, 2020a) and
b) EU Cybersecurity Strategy for the Digital Decade (European Commission, 2020b).

The EU Security Union Strategy, adopted on 24 July 2020, creates a general framework for cooperation in the field of internal security within the EU. It covers a wide spectrum of issues to be implemented for the years 2020–2025, from counteracting terrorism and organised crime to the protection of critical infrastructure, including transport and digital infrastructure. Its aim is to ensure that the Union is able to effectively respond to new, transboundary forms of threats, including those related to cyberattacks directed at air traffic management systems, airports, or satellite communications. The document indicates the need to develop mechanisms for exchanging information on security incidents between public and private institutions, as well as the need to integrate physical and digital security policies (Çelik et al., 2019).

The text of the strategy does not contain an explicit, detailed reference to the aviation sector as such in a leading or distinguished manner; however, it includes a reference to transport as a part of critical infrastructure. This should be understood to mean that airports, air traffic management systems, and ground handling may be treated as elements of this system. In the context of digital and hybrid threats, aviation is a sector strongly

dependent on internet communication networks and connectivity; therefore, the strategy may, in fact, be relevant (e.g., in the context of cyber threats directed at aviation systems). The second pillar of the European approach is the EU Cybersecurity Strategy, presented on 16 December 2020 by the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. This document defines the directions of actions aimed at building the cyber resilience of the European economy, protecting critical infrastructure, and strengthening cooperation between the public and private sectors.

In the strategy, it was clearly indicated that, in order to increase the level of cyber-resilience of all essential sectors, including air transport, the Commission introduced into the EU aviation security regulations provisions relating to cybersecurity, doing so through Commission Implementing Regulation 2019/1583 (European Commission, 2019). It was also confirmed that work would continue on strengthening the cybersecurity of the Galileo system in relation to the services of the European next-generation global navigation satellite system, as well as on developing security measures related to other components of the EU Space Programme.

In the strategy, it is underlined that in the aviation sector, given its cross-border nature and the complexity of its systems, cybersecurity should be treated as an integral part of Safety Management Systems. In this context, the establishment of Information Sharing and Analysis Centers (ISACs) is promoted, with the aim of enabling the continuous exchange of data on incidents and vulnerabilities between air carriers, airports, air navigation service providers and EU institutions such as EASA and ENISA (the European Union Agency for Cybersecurity).

In summary, both strategies have a common goal: increasing Europe's resilience to hybrid threats in which cyberattacks are used as a tool to destabilize the functioning of essential sectors of the economy and public security. Both initiatives also promote solutions based on artificial intelligence and real-time data analysis, which can be used for the early detection of incidents in aviation systems. In practice, this means that the civil aviation

sector is treated by the European Union as one of the pillars of common digital security, requiring coherent actions at the level of Member States and EU institutions.

An important element in implementing the strategies discussed is the adoption of Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, known as the NIS 2 Directive (Official Journal, 2022). This act establishes the legal framework for the protection of networks and information systems, also covering the civil aviation sector, which is recognized in Annex I, point 2 as a key sector (essential sector). In accordance with the provisions of the directive, all entities operating in civil aviation, including air carriers, airport operators, and operators providing air traffic control services (ATC), have been classified as essential entities. This means that they are obliged to meet specific requirements in the field of cybersecurity risk management and incident response.

Operators of critical infrastructure, including airports and airlines, must implement protective measures against cyberattacks, such as systematic security monitoring, risk analyses, and incident response mechanisms. This requirement arises directly from Article 21(1–2) of the NIS 2 Directive, which imposes on essential entities the obligation to implement adequate and proportional technical, operational, and organizational measures aimed at preventing and minimizing the effects of cyber incidents.

Article 10(1) of the NIS 2 Directive obliges Member States to establish national competent authorities for cybersecurity, responsible for coordinating the supervision of compliance with the Directive and the exchange of information on threats and incidents via the CSIRT Network (Computer Security Incident Response Team Network). At the same time, in order to prevent the overlapping of obligations and the emergence of regulatory gaps in the area of cybersecurity in aviation, the NIS 2 Directive provides for cooperation between national authorities responsible for aviation security operating on the basis of Regulations (EC) No 300/2008 and (EU) 2018/1139, and the competent cybersecurity authorities established under NIS 2. In accordance with Article 4(1) of the NIS 2 Directive, if an aviation-sector entity meets the security requirements laid down in

aviation regulations, including delegated and implementing acts adopted under the aforementioned regulations, its actions may be recognised by the competent cybersecurity authority as equivalent to the requirements of NIS 2. This solution is intended to prevent the duplication of obligations and reduce administrative burdens.

To strengthen information exchange and cooperation at the EU level, Article 14 of the Directive provides for the establishment of the Cybersecurity Cooperation Group. This body may invite representatives of EU institutions and agencies, such as Europol, the European Data Protection Board, EASA, or the EU Agency for the Space Programme (EUSPA), operating under Regulation (EU) 2021/696, to participate in its work. Their involvement is intended to enable effective coordination of actions and to enhance the resilience of aviation infrastructure to cyberattacks.

The implementation of the NIS 2 Directive in the aviation sector is therefore closely linked to the assumptions of the EU Security Union Strategy and the Cybersecurity Strategy of 16 December 2020. These documents promote actions aimed at increasing digital resilience through the development of innovation, the creation of specialised information-sharing centres (ISACs), and the development of public-private partnerships in the area of cyber-protection. It is worth noting that civil aviation is among the sectors particularly vulnerable to ransomware attacks and other forms of cyber threats, especially those affecting air traffic management systems. In the context of these conditions, building the digital resilience of civil aviation requires an approach combining legal regulations, technical standards, and broad international cooperation.

5. ROLE OF THE STATE IN BUILDING RESILIENCE TO CYBER THREATS IN CIVIL AVIATION

The role of the state in aviation cybersecurity is fundamental on many levels. The state fulfills it through its regulatory, supervisory, coordinating, and operational functions. The most fundamental is the regulatory function, which defines the rules for the functioning of state authorities and institutions, as well as other entities. Sidorkiewicz (2010)

expresses a similar view, emphasizing that creating good law strengthens internal order and stability, and consequently contributes to greater integrity (Sidorkiewicz, 2010, 221). The state acts as the main regulator in the field of cybersecurity in civil aviation within the boundaries of its territory. It creates and updates regulations, standards, and norms concerning cybersecurity in aviation, implementing the provisions and recommendations of international organizations into the national legal system.

Filinovych & Hu (2021) stress that in order to achieve the goal of ensuring universal cybersecurity in the field of aviation, it is necessary to combine efforts not only by air carriers but also by all actors interested in maintaining the quality and safety of flights, as well as by national governments (Filinovych & Hu, 2021, 120-126).

Properly constructed legal frameworks and the standardization of regulations enable the unification of security procedures and a rapid response to incidents. Therefore, state intervention, implemented among other things through the adoption of international standards and the coordination of cross-sectoral activities, constitutes the foundation for building the resilience of the entire aviation infrastructure. The effectiveness of these solutions depends on close cooperation with regulatory agencies such as EASA and ICAO, which define the operational and technical frameworks for cybersecurity systems. The supervisory function is no less important, as it serves as a mechanism for enforcing established regulations and standards. Regulations define the framework within which entities operate, whereas the supervisory function concerns their compliance, the detection of irregularities, and the introduction of corrective measures. Without effective supervision, regulations may remain merely a formality, failing to ensure a real level of security and operational effectiveness. State authorities responsible for oversight (e.g., the national civil aviation authority) must monitor whether aviation entities, such as air carriers, airports, and air traffic services, effectively implement the requirements for protection against cyber threats.

The coordination function enables effective information exchange between various entities operating within the state as well as between institutions and international

organizations in the field of cybersecurity. Thanks to such coordination, it is possible to quickly detect incidents, jointly develop procedures for responding to threats, and implement coherent protection strategies. This approach increases the resilience of the entire aviation system to cyberattacks, enabling not only prevention but also efficient and integrated crisis response. It is important to emphasize the dimension of international cooperation within this function. The state participates in various international organizations and initiatives aimed at developing the best standards for responding to threats in cyberspace.

The most practical dimension is the operational function, which reflects how the legal framework and preparedness for countering cyberattacks are implemented in reality and how effective they are. It has broad scope, as it covers the full spectrum of the cybersecurity management system. This applies not only to the technical dimension but also to the educational one. In practice, the state's operational function translates into the implementation of technological solutions, the delivery of training for personnel, and the development of cross-sector cooperation mechanisms, which make it possible to quickly identify threats and minimize the consequences of potential cyberattacks. Within this function, the state undertakes actions such as monitoring critical infrastructure, responding to cyber incidents, investing in modern technologies, and organizing training for personnel responsible for cybersecurity. As a result, the state's role becomes comprehensive, combining strategic, coordination, and operational aspects, which is essential for the effective protection of the civil aviation sector.

6. IDENTIFICATION OF DIGITAL THREATS

Due to technological development and the global use of IT systems in the civil aviation sector, it is necessary to properly manage these systems in order to ensure continuity of operations and safety. In the digital era, the management of aviation systems is largely automated, using solutions that enable remote monitoring and control. Maintaining constant access to information and communication (ICT) networks, both in ground

infrastructure and on board aircraft, is crucial for maintaining a high level of safety and minimising the risk arising from cyber threats. Madej and Terlikowski (2009) point out that individual systems are managed via ICT networks (Madej and Terlinkowski, 2009, 87).

In order for the state to effectively secure the civil aviation sector against cyber threats, it is necessary to create an appropriate cybersecurity management system. Similarly, the protection of sensitive data, such as passenger information or operational data, must be a priority. ICT networks play a paramount role here, as they are the foundation of the functioning of critical aviation infrastructure—from air traffic management systems, through on-board systems, to ground infrastructure (Bayram et al., 2022).

The high dependence of civil aviation on ICT systems implies many threats. As M. Szczepaniuk notes, in the coming years increasingly broad areas of civil aviation activity will be critically dependent on the reliable and secure functioning of ICT systems (Szczepaniuk, 2023, 110). All systems related to the safety of flight operations, including navigation services and onboard systems in aircraft, as well as air traffic management systems, must be thoroughly secured and resistant to cyberattacks. Any weakness in a single link can cause enormous losses not only in material terms, but also in human and environmental terms. Threats in the digital space in civil aviation are similar for all entities. The distinguishing factor is the scale and the entity concerned. ICT security systems are adjusted to the appropriate level of risk assessment and threats in a given entity. Therefore, the first step in identifying threats is an audit and assessment of the current state of security measures. All potential weaknesses must be identified, in particular outdated software, configuration errors, or gaps in the security of operating systems. It is also important to carry out simulations of cyberattacks, as this makes it possible to assess the extent to which the current protective measures are able to counter modern attack techniques.

7. THREATS ASSOCIATED WITH THE USE OF DRONES IN PUBLIC SPACES

The drone market, which has many useful and lawful applications, is constantly developing. These devices can be used, among other things, in transport, rescue operations, precision agriculture, environmental monitoring, and the activities of law enforcement agencies. At the same time, however, they may be used by criminals and terrorists for unlawful purposes. As G. Zając points out, one of the significant threats to the development of modern aviation technologies is the lack of comprehensive regulations and insufficient awareness of the need to comply with applicable standards and rules (Zając, 2021, 62). Moreover, as Ben Nassi et al. (2019) point out, drones generate new threats to security and privacy in society — including the possibility of their uncontrolled use, the lack of adequate methods for detection and mitigation, and research gaps in the field of security technologies (Ben Nassi, 2019, 1434). Tubis et al. (2024), in the publication *Risks of Drone Use in Light of Literature Studies*, conducted a systematic literature review on the risks associated with the use of drones. They indicated, among other things, that there are clear methodological gaps in the assessment of drone risk in various applications and that the growing number of drone operations in public space requires a comprehensive approach (Tubis et al, 2024, 3).

Public spaces are particularly vulnerable to attacks carried out with the use of drones. Such attacks may be directed against individuals, gatherings, critical infrastructure, law enforcement authorities, state borders or open areas. The response to these challenges are the regulations developed by EASA and adopted by the European Commission in the years 2019–2021, which constituted an important first step towards harmonising the rules on the use of unmanned aircraft in the EU. These regulations concern, inter alia:

a) registration of drone operators (Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft) (Official Journal, 2019a),

b) the obligation to use direct remote identification for unmanned aircraft (Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems) (Official Journal, 2019b),
c) classification of operations according to the level of risk (Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing the European Union Aviation Safety Agency (the so-called *Basic Regulation*) (Official Journal, 2018).

In accordance with Article 14(1) of Regulation 2019/947, every operator carrying out operations in the "open" or "specific" category is required to register in the national register of UAS operators maintained by the competent authority of the Member State. It is worth explaining that the "open" category covers operations conducted under low-risk conditions, which do not require prior authorisation from the competent authority or a declaration by the operator. Pursuant to Article 4(2) and Annex, Part A, such operations may be conducted provided that a number of limitations are met, including, among others: flight within the pilot's visual line of sight (VLOS), a maximum flight height of 120 metres above ground level, and a prohibition on the carriage of persons or dangerous goods. By contrast, the "specific" category covers operations with a medium level of risk, which do not fall within the scope of the open category. According to Article 5(1), before carrying out such an operation the operator must obtain an authorisation issued by the competent authority of the Member State, based on an operational risk assessment (*Specific Operations Risk Assessment* – SORA).

The registration requirement referred to above also applies to remote pilots who operate drones equipped with a remote identification system or capable of causing serious injury in the event of a collision. As part of the registration process, the operator is assigned a unique registration number which, in accordance with Article 14(5)–(7), must be entered into the drone's remote identification system. This ensures that the user's identity can be verified immediately in the event of an incident or breach of the regulations.

Registration is electronic and harmonised across the European Union, which means that data from national registers are interoperable and available to other Member States through an information-sharing system managed by EASA. The introduction of a single register of operators has been a fundamental element in building a common European market for drone operations, enhancing both the safety of the airspace and the effectiveness of administrative oversight.

In accordance with Regulation (EU) 2019/945, unmanned aircraft falling within certain classes (C1, C2, C3)[1] must be equipped with a direct remote identification system. This system continuously broadcasts identification data, including, among others, the operator's registration number, the drone's position, the remote pilot's position and the device's serial number. This information can be received by other entities within transmission range, such as law-enforcement agencies, aviation authorities or other airspace users.

In the field of unmanned aircraft regulation, Regulation (EU) 2018/1139 is of key importance for ensuring their safe operation. It establishes the legal framework for the functioning of EASA in the area of aviation safety, including cybersecurity. As stipulated in Article 88(1) of Regulation 2018/1139, the Commission, EASA and the Member States are required to cooperate in the field of civil aviation security, including cybersecurity, particularly where there are interdependencies between safety and security. These provisions are designed to ensure a coherent EU-wide approach to aviation cybersecurity, helping to avoid gaps in protection in the context of international air operations.

In accordance with Annex IX, point 1.1 of Regulation (EU) 2018/1139, the operator and the remote pilot of an unmanned aircraft are required to ensure that operations are conducted safely and responsibly, with due regard for rules on safety, the protection of privacy and personal data, civil liability, insurance, civil protection and the natural environment. They are required to be familiar with the manufacturer's operating

[1] These classes distinguish drones, among other things, by maximum take-off mass, maximum operating speed, flight altitude, geofencing requirements, noise emission levels, and whether they must be equipped with a direct remote identification system.

instructions, to make proper use of the aircraft's functions, and to comply with the applicable rules of the air and air traffic management/air navigation services (ATM/ANS) procedures. These provisions indicate that the operation of UAS must guarantee safe separation from people and from other airspace users, and that the design and handling of the aircraft should eliminate the risk of exposing people to danger (Annex IX, point 1.2). On the basis of these principles, EASA has developed a framework model for classifying drone operations according to their level of risk, which was subsequently elaborated in implementing rules, in particular in Regulation (EU) 2019/947. This model distinguishes three main categories of operations: "open", "specific" and "certified", corresponding respectively to low, medium and high levels of risk. This approach constitutes an important element of the European drone safety system, combining technical, procedural and organisational requirements with the principle of proportionality to the degree of operational risk (Ayçiçek et al., 2021).

However, further action is still required, as in the third decade of the 21st century drones are becoming increasingly accessible. Additional measures could include enhanced information sharing, the development of guidelines and best practices for widespread use, including by law enforcement authorities, as well as broader testing of counter-drone measures. It is also necessary to examine in greater detail issues of privacy and data protection in the context of the use of drones in public spaces.

CONCLUSION

Civil aviation, in the era of advancing digitalization, has become a sector critically dependent on the security of information and communication technology (ICT) systems, which makes it particularly vulnerable to cyber threats. These threats, ranging from external attacks to internal irregularities, can disrupt the functioning of aviation operational systems such as air traffic control or ground traffic management.

In the course of the analysis, it was established that civil aviation, in a period of intensive digitalization, has become critically dependent on the reliability and security of ICT systems, which makes it exceptionally exposed to cyber threats.

International regulations play a crucial role in building resilience. ICAO has created global cybersecurity standards (including through Annex 17 to the Chicago Convention and the guidance contained in Doc 9985), obliging member states to protect aviation systems and to develop cooperation mechanisms. It should be emphasized that the policy directions set out in the strategies demonstrate the need for proactive risk management, with a focus on developing cyber resilience at every institutional level. At the European level, the EU Cybersecurity Strategy and the NIS 2 Directive (which classifies aviation as an essential sector) impose on air carriers, airports and air traffic control (ATC) services the obligation to implement adequate risk management and incident response measures, while states themselves perform a supervisory role. The role of the state is fundamental and is carried out through regulatory, supervisory, coordinating and operational functions.

The research hypothesis, assuming that effective resilience can be achieved through the comprehensive integration of global and regional standards and the synergistic use of state functions, has been positively verified.

An additional challenge is the growing risk associated with the use of drones in public spaces, which requires further standardization and testing of protective measures. EASA and European Commission regulations have already established a framework for operator registration, remote identification and the classification of operations according to risk (categories: open, specific).

In conclusion, effective protection of the civil aviation sector requires a holistic and integrated approach that combines close international cooperation, the continuous updating of legal regulations and the development of a widespread cybersecurity culture.

REFERENCES

Ayçiçek, S., Öz, S., (2021). Fair Logistics, Journal of Industriaal Policy and Technology Management (JIPAT), 4(1), pp. 11-25.

Bayram, S., Öz, S., Ekmekci, İ., (2022). Metaverse platformlarında siber güvenliğe yönelik yaklaşımlar, Chapter in the Book: Metaverse, Saabri Öz, Rızvan Yılmaz, Cengiz Akyıldız, İstanbul, Hiperyayın, pp. 163-191.

Çelik, F.B., Avşar, B., Öz, S., (2019). Structural Investigation of Project Logistics and Transportation, Journal of Industriaal Policy and Technology Management (JIPAT), 2(1), pp. 13-22.

European Commission. (2019). *Commission Implementing Regulation (EU) 2019/1583 of 25 September 2019 amending Implementing Regulation (EU) 2015/1998 laying down detailed measures for the implementation of the common basic standards on civil aviation security with regard to cybersecurity measures* (OJ L 246, 15–18).

European Commission. (2020a). *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Security Union Strategy* (COM(2020) 605 final).

European Commission & European External Action Service. (2020b). *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade* (JOIN(2020) 18 final).

European Parliament & Council of the European Union. (2021). *Regulation (EU) 2021/696 of 28 April 2021 establishing the Union Space Programme and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision No 541/2014/EU* (OJ L 170, 69–148).

Filinovych, V., & Hu, Z. (2021). Aviation and the cybersecurity threats. In *Advances in Economics, Business and Management Research* (Vol. 188, pp. 120–126). https://doi.org/10.2991/aebmr.k.210826.021

Madej, M., & Terlikowski, M. (2009). *Teleinformation security of the state*. Polish Institute of International Affairs.

Nassi, B., Bitton, R., Masuoka, R., Shabtai, A., & Elovici, Y. (2021). SoK: Security and privacy in the age of commercial drones. In *2021 IEEE Symposium on Security and Privacy (SP)* (p. 1434). IEEE.

Official Journal of the European Union. (2018). *Regulation (EU) 2018/1139 of the European Parliament and of the Council of 14 August 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending various aviation-related regulations and directives* (OJ L 212, 1–122).

Official Journal of the European Union. (2019a). *Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft* (OJ L 152, 1–40).

Official Journal of the European Union. (2019b). *Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft and on third-country operators of unmanned aircraft systems* (OJ L 152, 45–71).

Official Journal of the European Union. (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive) and repealing Directive (EU) 2016/1148* (OJ L 333, 80–152).

Sidorkiewicz, K. (2010). Contemporary approaches to the functions of the state. *Studia Elbląskie, 11*, 215–229.

Szczepaniuk, E. (2023). Selected aspects of cybersecurity in civil aviation. *Aviation and Security Issues, 3*(1/2023), 110.

Tubis, A. A., Poturaj, H., Dereń, K., & Żurek, A. (2024). Risks of drone use in light of literature studies. *Sensors, 24*(4), 1205.

Ukwandu, E., Ben-Farah, M., Hindy, H., Bures, M., Atkinson, R., Tachtatzis, C., Andonovic, I., & Bellekens, X. (2022). Cyber-security challenges in the aviation

industry: A review of current and future trends. *Information, 13*(3), 146. https://doi.org/10.3390/info13030146

Zając, G. (2021). Advancement of unmanned aircraft machines applications for aviation safety and global marketplace. In *Technology Management and Industrial Policy* (Vol. 1, pp. 62). Istanbul, Turkey.