UDC 341.226
DOI https://doi.org/10.32850/LB2414-4207.2020.16.04

THE ROLE OF INTERNATIONAL ORGANIZATIONS IN THE DEVELOPMENT OF INTERNATIONAL COOPERATION IN THE FIELD OF CIVIL AVIATION CYBERSECURITY

Holik Yuliia Olehivna,
Postgraduate Student at the European Union Law Department
(Yaroslav Mudryi National Law University, Kharkiv, Ukraine)

The Article is devoted to the enlightenment of the evolution of the role of international cooperation in the civil aviation cybersecurity within the frameworks of some international organizations. The history and the key features of such cooperation deepening are addressed. Due attention is given to the main developmental milestones of cooperation and contributions of international organizations to this process. Albeit the main United Nations aviation agency (ICAO) referred to the cybersecurity matter back in 2009, the primary documentary development in the sphere is the result of an aviation conference held by the American Institute of Aeronautics and Astronautics. Later on, the International Civil Aviation Organization has stepped in with plans, strategies, declarations and resolutions adopted on numerous conferences of aviation and security. Moreover, it takes part in the Industry High-Level Group, which unites five universal organizations of the civil aviation industry. Having different legal nature and spheres of influence, they agreed upon the alignment of cooperative actions concerning cyber threats to this extensively computerized system. In particular, the International Air Transport Association coordinates global efforts in the detection and assessment of cyberattacks risks. In its turn, the Civil Air Navigation Services Organization is an intermediary for industry companies that provides communication between them and promotes the exchange of relevant information. Regional organizations keep up with a great job of development of a stable and attacks-resilient global framework. For instance, the European Union Aviation Safety Agency elaborates on the safe sky across the territory of the European Union and beyond. Overall, civil aviation cybersecurity is a sphere of international interaction involving both international and national stakeholders that take into consideration both legal and technical approaches.

Key words: civil aviation, cybersecurity, civil aviation cybersecurity, international cooperation, international law cooperation, evolution of cooperation mechanisms.

РОЛЬ МІЖНАРОДНИХ ОРГАНІЗАЦІЙ У РОЗВИТКУ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У СФЕРІ КІБЕРБЕЗПЕКИ ЦИВІЛЬНОЇ АВІАЦІЇ

Голік Юлія Олегівна,
аспірантка кафедри права Європейського Союзу
(Національний юридичний університет імені Ярослава Мудрого,
м. Харків, Україна)

Статтю присвячено висвітленню еволюції ролі міжнародної співпраці в забезпеченні кібернетичної безпеки цивільної авіації в рамках деяких міжнародних інституцій. Досліджено історію та визначено ключові особливості розвитку такого

співробітництва. Належну увагу приділено основним етапам розвитку співробітництва й впливу міжнародних організацій на цей процес. Хоча головна авіаційна установа Організації Об'єднаних Націй – Міжнародна організація цивільної авіації (ІКАО) – звернулася до питання кібербезпеки в цивільній авіації ще у 2009 році, перше документальне розроблення в цій сфері стала результатом роботи конференції з питань авіації, яку організувала національна установа – Американський інститут аеронавтики та космонавтики. Пізніше ІКАО ухвалювала плани, стратегії, декларації й резолюції на численних конференціях з авіації та безпеки. Вона бере активну участь у роботі Галузевої групи високого рівня (Industry High-Level Group), членами якої є п'ять універсальних організацій індустрії цивільної авіації. Різні за правовим статусом і сферою впливу на галузь, вони домовилися про спільну програму погодження спільних дій щодо кібернетичних загроз цій комп'ютеризованій системі. Зокрема, Міжнародна асоціація повітряного транспорту (IATA) координує глобальні зусилля авіакомпаній із виявлення й оцінювання ризику кібератак. Цивільна організація аеронавігаційного обслуговування (CANSO) зі свого боку є посередником для галузевих компаній, забезпечуючи зв'язок між ними й обмін релевантною інформацією. Однак регіональні організації проводять не меншу за обсягом і значенням роботу з розбудови стабільної та стійкої до атак глобальної системи цивільної авіації, ніж універсальні. Так, Агенція авіаційної безпеки Європейського Союзу опікується питаннями безпечного неба на території Європейського Союзу та за його межами. Отже, кібернетична безпека цивільної авіації – та сфера міжнародної взаємодії, у якій важливі внески як міжнародних, так і національних установ, котрі враховують позиції як правового, так і технічного характеру.

Ключові слова: цивільна авіація, кібербезпека, кібербезпека цивільної авіації, міжнародне співробітництво, міжнародно-правове співробітництво, еволюція механізмів співробітництва.

Civil aviation is a global, borderless, extensively computerized industry. The scope of computer systems maintaining the lines of supply in the aviation industry embraces air navigation systems, onboard aircraft control and communication systems, airport ground systems, flight information systems, etc. In the environment heavily reliant on digitalization, potential insecurities are at the highest point. Cybersecurity of airport and aircraft operations is aviation cybersecurity.

To address issues of civil aviation comprehensively and coherently, stakeholders of different levels (global, regional, national) should work together and develop a stable and attacks-resilient global framework. The cooperation aims for prevention, detection, removal and recovery from the attacks on the aviation networks [1, p. 3] and takes various forms: running joint projects, organization of professional fora, common strategies drafting and implementation control.

For the expansive view on the issue of civil aviation cybersecurity, in this Article we are referring to international cooperation in any form regardless of its parties and their status. Mainly, international cooperation in the sphere of civil aviation cybersecurity takes place under the auspices of international intergovernmental organizations concerned with civil aviation matters. Nevertheless, other organizations, agencies and companies also contribute to the enhancement of the level of cybersecurity protection through the development of intergovernmental and intercorporate relations. It is "a cohesive interest" of the multitude of disparate stakeholders within the aviation ecosystem to ensure continuous operation of the cybersecurity strategy and framework. The problem of one stakeholder may have spillover effects on the industry. Thus, cyber-risk governance should be collective and coordinative. Reflecting the part that the level of threat sophistication is rapidly growing.

Attention to the issues is growing and researchers focus on different aspects of it: international aviation law (R. Abeyratne, R.Bartsch, M. Pearson, D. Riley), general security of flights (N.V. Zhmur), cybersecurity (A.V. Paziuk, D.V. Dubov, M.N. Schmitt), cybersecurity in civil aviation (E. Papadopoulos, E. Sils). Nevertheless, science lacks comprehensive research on cooperation in the sphere of civil aviation cybersecurity.

Keeping up with the history of the deepening of collaboration between civil aviation stakeholders, we are going to focus on the main achievements regarding cybersecurity issues of some international organizations.

The International Civil Aviation Organization (hereinafter – ICAO) laid the foundation stone in 2009 and amended Annex 17 relating to security with the relevant provision on civil aviation cybersecurity in 2012. Nevertheless, the first document on the matter was approved in 2013 under the auspices of a national. The American Institute of Aeronautics and Astronautics (AIAA) held the AVIATION 2013 conference, that resulted in a roadmap for the global aviation cybersecurity framework – "The Connectivity Challenge: Protecting Critical Assets in a Networked World: a Framework for Aviation Cybersecurity". It encompassed steps for cybersecurity governance that later were upheld and upgraded by others. Moreover, it underlined "a shared responsibility, involving governments, airlines, airports, and manufacturers" of resisting cyber threats [2]. Thus, these stakeholders should collaborate and build industry resilience by the establishment of common cyber standards and culture for aviation systems, work on the common understanding of threats and risks, communication of the threats and assurance situational awareness, provision of incident response, strengthening of the defensive system, conduct of necessary research and development.

ICAO as a universal organization specializing in aviation has a great value for the encouragement of collaboration among the civil aviation industry stakeholders. Hence, it simultaneously serves as both one of the biggest fora and the most influential stakeholders.

The issue of cyber threats stood in the spotlight of ICAO's attention in 2009. At the Twentieth Meeting of the ICAO Aviation Security Panel (hereinafter – the AVSEC Panel), the European Civil Aviation Conference underlined the vulnerability of civil aviation cybersecurity. The Panel considered the amendment of Annex 17 (a compilation of the Standards and Recommended Practices (SARPs) concerning aviation security) with the relevant provisions [3, p. 19]. Later on, alike issues were raised and addressed in September 2012 (the ICAO High-level Conference on Aviation Security), October 2012 (the 12th ICAO Air Navigation Conference) until Annex 17 was amended by a new Recommended Practice. Albeit Rule 4.9 of Annex 17 (concerning Security Standards) refers to preventive security measures in the sphere of cybersecurity, it does not contain the term "cybersecurity". It focuses on the national states' obligation to develop appropriate measures for the protection of civil aviation information and communication technology systems. Thus, this provision lacks interstate collaboration.

In September 2013, the ICAO Secretary General initiated the creation of the Industry High-Level Group (hereinafter – the IHLG). It is an informal group uniting the Heads of five universal civil aviation industry organizations: ICAO, the Airports Council International (ACI), the Civil Air Navigation Services Organization (hereinafter – CANSO), the International Air Transport Association (hereinafter – IATA) and the International Coordinating Council of Aerospace Industries Associations (ICCAIA). Since December 5, 2014, these organizations have a common roadmap for the alignment of cooperative actions concerning cyber threats – the Civil Aviation Cybersecurity Plan. It recalls and upgrades the roadmap suggested earlier. Albeit being concrete, this Plan is neither legally binding nor actions restricting upon members for participation in other efforts aiming at the protection

of civil aviation. Moreover, flexibility is the principle of this cooperation. Various steps (short-, mid- and long term) encompass joint work, information sharing, public promotion [4, p. 3–5].

In September-October 2016 (during the 39th session), the ICAO Assembly addressed civil aviation cybersecurity matters and called upon states and industry to work on it extensively in a coordinated manner (Resolution A39-19 "Addressing Cybersecurity in Civil Aviation"). Recommendations provided recall the ideas submitted in the IHLG Civil Aviation Cybersecurity Action Plan [5, p. VII-23].

In April 2017, ICAO organized an inaugural Cyber Summit and Exhibition civil aviation cybersecurity in Dubai, United Arab Emirates. Paragraph 3 of the Dubai Declaration on cybersecurity in civil aviation emphasizes the crucial (*sine qua non*) character of the "collaboration and exchange between states and other stakeholders" for the "development of an effective and coordinated global framework" [6].

Meanwhile, the Global Aviation Security Plan (GASeP) adopted in November 2017 superseded the ICAO Comprehensive Aviation Security Strategy agreed upon in 2011. Cooperation is both the separate goal and the underlying principle of GASeP priority outcomes. Moreover, the Global Air Navigation Plan 2016-2030 (GANP) emphasizes the importance of strong cybersecurity for global aviation information management [7, p. 113].

In March 2018, the ICAO Council adopted Amendment 16 to Annex 17 suggested by the 2017 AVSEC Panel. It has not only changed the 4.9.1. Standard, but also suggested a recommendation 4.9.2. Still, cooperation is not directly stated but rather implied. They are applicable from 16 November 2018.

In May 2018, ICAO Europe, Middle East and Africa held a summit on Cybersecurity in Civil Aviation in Bucharest, Romania. In the Bucharest communique, cross-disciplinary cooperation is a crucial element for the addressing of cyber challenges in the aviation industry.

Finally, ICAO Assembly Resolution A40-10 (October 2019) "Addressing Cybersecurity in Civil Aviation" contains the encouragement upon states and industry stakeholders to implement the adopted ICAO Cybersecurity Strategy.

Among the seven pillars forming the basis of the Strategy, international cooperation comes first. It suggests ICAO serve as a forum for states, international organizations and industry representatives to effectively address international civil aviation cybersecurity through discussions, summits, exhibitions, workshops, etc. However, it would be wrong to state that only the first pillar of the Strategy encompasses international cooperation. Some others also contain elements supposing an active interaction between states. In particular, such stipulations are implied within paragraphs 2.2 and 2.3 (Governance), 3.4 (Effective legislation and regulation), 5.2 (Information sharing), 6.2 (Incident management and emergency planning) [8].

It is worth noting that states are primary subjects of the Strategy. "Industry stakeholders" come up in the "Governance" part only in the context of the need for coordination channels to be established (Paragraph 2.2). "Industry" is mentioned in the "International Cooperation", "Effective Legislation and Regulation" and "Capacity Building, Training and Cybersecurity Culture". However, the call for action in Resolution A40-10 addresses both states and industry stakeholders.

Therefore, the International Civil Aviation Organization works actively on the international cooperation extension through establishing working groups, adopting relevant provisions, organizing international events and serving as a platform for the interaction of states, organizations and other stakeholders involved in the sphere.

One of such stakeholders is the International Air Transport Association (IATA) that serves the needs of airlines. It assists in the development of effective cybersecurity strategies and drives "coordination of global efforts to address cyber threats to aviation" [9]. IATA elaborates on cybersecurity issues through identification and evaluation risk of a cyber-attack, defining information-sharing mechanisms and advocating for regulations and cooperation in the industry.

On the Civil Aviation Cyber Security Conference in Singapore held on 8 July 2015 (organized by Singapore in partnership with ICAO and IATA), IATA's Director General and CEO Tony Tyler emphasized two opportunities for the efficient address of cyber threats: a governmental partnership with the private sector and stakeholders' collaboration. As regards the latter, it is based on the exchange of operational and air traffic information [10].

Another important contributor to aviation security is the Civil Air Navigation Services Organization (CANSO). It organizes international events that foster professional dialogue: annual World air traffic management (hereinafter – ATM) congresses, regional conferences, symposiums, summits, ATM weeks and gala-dinners, workgroup meetings, workshops.

It also produced CANSO Cyber Security and Risk Assessment Guide (2014) encouraging close multi-stakeholder cooperation within and outside the organisation through large-scale information sharing and industry collaboration. Interaction between stakeholders is a key component of each of the four-tier cybersecurity maturity system (partial, risk-informed, repeatable and adaptive) [11, p. 18–23].

In parallel, the alike job has been done on a regional level. In 2013, the European Commission (an institution of the European Union) listed cyber-attacks on civil aviation among risks that should be addressed by civil aviation security [12, p. 5].

Agency responsible for civil aviation issues within the EU is the European Union Aviation Safety Agency (hereinafter – EASA). It serves the safe air travel maintenance in Europe, works on the establishment, development of and compliance with safety and security standards within the borders of the European Union.

In 2016, it defined elaboration on a roadmap to address cybersecurity threats with the European Commission, EU Member States and industry as one of its key actions (Action numbers SPT.071 – Safety Promotion, RMT.0648 – Rulemaking) in the European Aviation Safety Plan 2016–2020 [13, p. 4]. Besides, EASA included international cooperation in the produced "Bucharest Declaration on high-level efforts in civil aviation cybersecurity" (November 2016). It represents the coordinated European approach and focuses on information sharing, reporting, internationally harmonized regulations, risk assessments, promotion, knowledge and foresight.

Moreover, EASA and the Computer Emergency Response Team of the EU Institutions (the CERT-EU) established the European Centre for Cyber Security in Aviation (hereinafter – the ECCSA; Action number SPT.072) [13, p. 43]). It covers the full spectrum of aviation consultation services.

In 2018, new tasks were introduced: drafting of regulation for cybersecurity risks (Action number RMT.0720) [14, p. 58] and aeronautical vulnerabilities database development (Action number RES.012 – Research) [14, p. 59].

In September 2019, the first issue of the Strategy for Cybersecurity in Aviation was published under the auspices of the European Strategic Coordination Platform (representatives of the European Commission, relevant European agencies and organizations, Member States, industry associations and worldwide regulatory partners and military organizations took part in drafting) [15, p. 70]. It is built upon ICAO Resolution A39-19 and mindful of the need to be reviewed according to Resolution A40-10 (as it has been adopted shortly before the 40th Session of ICAO) [16, p. 1]. The Strategy reveals challenges aviation cybersecurity is

facing, exposes identified gaps and difficulties for both civil and military spheres. It accepts the need for the required changes to support cooperation and information sharing [16, p. 4].

Not only states are engaged in civil aviation cybersecurity matters in the EU, but also aviation experts and various corporate elements [17]. Due to the interdependence of stakeholders, eligible organizations and actors are invited to become active players of the information-sharing network and the ECCSA.

As of the practical aspects of cooperation, the EU provides training for cybersecurity professionals. For instance, in 2018 the Cyber Europe training was devoted to aviation matters. In general, moot incidents let stakeholders not only be aware of the latest cyber threats but also help to elaborate on up-to-date legislative base.

Thus, with the particular character of international cooperation in the field of civil aviation cybersecurity, institutional mechanisms possess an unprecedented variety of the parties involved in the process. Moreover, international cooperation between various stakeholders is the *sine qua non* for the effective functioning of the global civil aviation cybersecurity framework. It is constantly being reaffirmed by international documents (Dubai Declaration, Bucharest Communique, the IHLG Civil Aviation Cybersecurity Action Plan, the ICAO Cybersecurity Strategy, the European Strategy for Cybersecurity in Aviation) and official positions of the stakeholders (states – Belgium, France, the United Kingdom, Romania; organizations – ICAO, IATA, CANSO; companies – Boeing, AIRBUS).

Being realised through different mechanisms, cooperation in the civil aviation industry is gaining momentum nowadays. Such mechanisms are working groups within international organizations (ICAO, EASA), international events putting together representatives of aviation and cybersecurity spheres from different circles (governmental, business, technical, etc.) – summits, workshops, conferences. Ways to cooperate do vary significantly: from the formulation of the common language to mutual cultural exchange between aviation and cultural industries.

In addition, the character of the industry requires a wide involvement of different contributors. Apart from traditional international law approaches, not only states and international intergovernmental organizations have a considerable impact on the process of addressing cyber risks, but also non-governmental organizations, companies and groups of experts.

References:

1. The Boeing Company. Views on the Framework for Improving Critical Infrastructure Cybersecurity. *National Institute of Standards and Technology Request for Information* (9 February 2016). URL: https://www.nist.gov/system/files/documents/2017/02/13/20160208_boeing.pdf (Last accessed: 26.04.2020).

2. The Connectivity Challenge: Protecting Critical Assets in a Networked World, a Framework for Aviation Cybersecurity. AIAA Decision Paper. *AIAA:* the World's Forum for Aerospace Leadership (August 2013).

3. Abeyrathe R. Aviation Security Law. Heidelberg : Springer-Verlag Berlin Heidelberg, 2010. 287 p.

4. Civil Aviation Cybersecurity Action Plan. URL: https://www.icao.int/cybersecurity/SiteAssets/ICAO/Civil%20Aviation%20Cybersecurity%20Action%20Plan%20-%20SIGNED.pdf (Last accessed: 26.04.2020).

5. Assembly Resolutions in Force (as of 6 October 2016). Doc 10075. *ICAO.* Montréal : International Civil Aviation Organization, 2017. URL: https://www.icao.int/Meetings/a39/Documents/Resolutions/10075_en.pdf (Last accessed: 26.04.2020).

6. Declaration on Cybersecurity in Civil Aviation. Dubai, 5 April 2017. URL: https://www.icao.int/Meetings/CYBER2017/Documents/Final%20text%20Declaration%20(2).pdf (Last accessed: 26.04.2020).

7. Global Air Navigation Plan 2016-2030. *ICAO.* Montréal : International Civil Aviation Organization, 2016. URL: https://www.icao.int/airnavigation/Documents/GANP-2016-interactive.pdf (Last accessed: 26.04.2020).

8. Aviation Cybersecurity Strategy: Security and Facilitation Strategic Objective. *ICAO.* Montréal : International Civil Aviation Organization, 2019. URL: https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf (Last accessed: 26.04.2020).

9. Addressing Cyber Security Challenges. *IATA* : web-site. URL: https://www.iata.org/en/about/worldwide/asia_pacific/Cyber-Security-Challenges/ (Last accessed: 26.04.2020).

10. Remarks of Tony Tyler at the 2015 Civil Aviation Cyber Security Conference, Singapore. *IATA* : web-site. URL: https://www.iata.org/en/pressroom/speeches/2015-07-09-01/ (Last accessed: 26.04.2020).

11. CANSO Cyber Security and Risk Assessment Guide. *CANSO*. 2014. URL: https://www.canso.org/sites/default/files/CANSO%20Cyber%20Security%20and%20Risk%20Assessment%20Guide.pdf (Last accessed: 26.04.2020).

12. 2012 Annual Report on the Implementation of Regulation (EC) N° 300/2008 on Common Rules in the Field of Civil Aviation Security: Report from the Commission to the European Parliament and the Council. *European Commission.* 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013DC0523&from=EN (Last accessed: 26.04.2020).

13. The European Plan for Aviation Safety 2016–2020. *European Aviation Safety Agency*. 2016. URL: https://www.easa.europa.eu/sites/default/files/dfu/EPAS%202016-2020%20FINAL.PDF (Last accessed: 26.04.2020).

14. The European Plan for Aviation Safety 2018–2022. *European Aviation Safety Agency*. 2017. URL: https://www.easa.europa.eu/sites/default/files/dfu/EPAS_2018-2022%20v2.2.8%20for%20MB.pdf (Last accessed: 26.04.2020).

15. The European Plan for Aviation Safety 2019–2023. *European Aviation Safety Agency*. 2018. URL: https://www.easa.europa.eu/sites/default/files/dfu/EPAS_2019-2023%20final.pdf (Last accessed: 26.04.2020).

16. Strategy for Cybersecurity in Aviation. *European Strategic Coordination Platform*. 2019. URL: https://www.easa.europa.eu/sites/default/files/dfu/Cybersecurity%20Strategy%20-%20First%20Issue%20-%2010%20September%202019.pdf (Last accessed: 26.04.2020).

17. Eligible organizations invited to join cybersecurity group ECCSA. *EASA* : web-site. URL: https://www.easa.europa.eu/newsroom-and-events/news/eligible-organisations-invited-join-cybersecurity-group-eccsa (Last accessed: 26.04.2020).