International cyber security strategy as a tool for comprehensive security assurance of civil aviation security: methodological considerations

Oleksandr Grygorov[1], Albina Basysta[2], Roman Yedeliev[3], Andrii Paziuk[4], Zakhar Tropin[5]
alexgrygorov@gmail.com
albinabasistaya@gmail.com
iedeliev@gmail.com
AndriiPaziuk74@gmail.com
zakhar.tropin@gmail.com dok.melnuchyk83@ukr.net
[1]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[2]Institute of International Relations of the Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[3]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine
[4]Kyiv Taras Shevchenko National University, Kyiv, Ukraine
[5]Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Summary
Civil aviation cybersecurity challenges are global in nature and must be addressed using global best practices and the combined efforts of all stakeholders. This requires the development of comprehensive international strategies and detailed plans for their implementation, with appropriate resources. It is important to build such strategies on a common methodology that can be applied to civil aviation and other interrelated critical infrastructure sectors. The goal of the study was to determine the methodological basis for developing an international civil aviation cybersecurity strategy, taking into account existing experience in strategic planning at the level of international specialized organizations. The research was conducted using general scientific and theoretical research methods: observation, description, formalization, analysis, synthesis, generalization, explanation As a result of the study, it was established the specifics of the approach to formulating strategic goals in civil aviation cybersecurity programs in the documents of intergovernmental and international non-governmental organizations in the aviation sphere, generally based on a comprehensive vision of cybersecurity management. A comparative analysis of strategic priorities, objectives, and planned activities for their implementation revealed common characteristics based on a single methodological sense of cybersecurity as a symbiosis of five components: human capacity, processes, technologies, communications, and its regulatory support. It was found that additional branching and detailing of priority areas in the strategic documents of international civil aviation organizations (by the example of Cybersecurity Strategy and Cybersecurity Action Plan) does not always contribute to compliance with a unified methodological framework. It is argued that to develop an international civil aviation cybersecurity strategy, it is advisable to use the methodological basis of the Cyber Security Index.

Key words:
cyber security, cyber defense, cyber preparedness, civil aviation, international strategy, regulatory support, international standards.

1. Introduction

The development of modern technologies, including in the aviation sphere, is accompanied by the introduction of a new type of threat - cyber threats to the security of air communications and air transport infrastructure - in the activities of civil aviation, is on several universal and specialized international organizations.

United Nations (UN) and several international aviation organizations, including the International Civil Association Organization (ICAO), the International Air Transport Association (IATA), the International Coordinating Council of Aerospace Industries Associations (ICAIA), European Organization for the Safety of Air Navigation (EUROCONTROL) direct their joint efforts to develop international standards for civil aviation cybersecurity as soon as possible, form the basic principles of future legal models of civil aviation cybersecurity at universal, regional and national levels.

Despite the significant relevance of the topic of aviation cybersecurity, the efforts of international aviation organizations can be characterized as insufficient for comprehensive cyber security in the planning and

Manuscript received September 5, 2021
Manuscript revised September 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.9.43

implementation of cyber and security programs for the civil aviation sector [20]. This necessitates synthesis of existing scientific and methodological approaches to the formation of cyber defense strategies, as well as a comparison of the priorities identified in the strategies of international aviation organizations and universal concepts of cyber preparedness assessment at the national level.

2. Literature review

At the present stage of development of air transportation to the topical issues of strengthening the security of civil aviation should be considered the problem of information security, received international recognition according to the relevant UN General Assembly resolution "Developments in the field of information and telecommunications in the context of international security" in 1999 [1]. According to Nashinets-Naumova [2], it was after the approval of this document, the issues of information security of civil aviation were recognized as a global challenge of our time. Based on this fact, several researchers of civil aviation cybersecurity issues, including Honcharova [3], argue that the establishment of strict regulation in this area is a consequence of a powerful supranational regulator in the field, namely ICAO.

Experts in the field of international air law consider cyber threats as one of the types of acts of unlawful interference with civil aviation. At the intersection of the topic of aviation security, combating terrorism, and cybercrime there is a range of issues that require a comprehensive approach, in particular with the use of international legal tools, as recalled by Klenka [4], Abeyratne [5] among others.

According to Silva [6], to reduce the risks of cyber-attacks and increase the resilience of the entire aviation ecosystem, a global approach, which will provide the necessary level of trust between the actors, is needed. It is worth remembering in this context EUROCONTROL, which deals with the security of air navigation, and emphasizes the importance of a comprehensive approach to the development of a trusted system of cyber security [7]. Organizational and technical issues of building cyber security systems for civil aviation infrastructure is one of the key issues on the agenda both at the level of subjects of aviation activity, and regulators at the state and supranational levels. The need to introduce a unified cyber security policy for aviation cyber-physical systems is noted in the works of Abeyratne [8], Alrefaei et al. [9], Nickolaos Koroniotis [10], Pollack and Ranganathan [11]. A unified framework based on risk assessment and management to address security threats and increase the resilience of aviation systems to future attacks is proposed by Lykou et al. [12].

Despite the existing vulnerability of civil aviation computer systems, ICAO has already made many attempts to develop cooperation among key stakeholders to identify cyber risks and minimize them. In addition, ICAO calls for clear management of civil aviation cybersecurity and appropriate measures to prevent cyber-attacks [13].

One cannot but agree that without a certain level of trust and goodwill of all involved participants to exchange information important for prevention and response to cyber incidents, it will be extremely difficult, if not impossible, to achieve results, as noted by Abeyratne [14], Jeyakodi [15], Lim [16], Pierides [17]. At the operational level, rapid incident response is an integral part of the cyber incident management process, in particular, the exchange of response-critical information should be provided by aviation-specific Computer Security Incident Response Teams (CSIRTs). The issue of unification of rules and approaches in the work of aviation CSIRT teams on the example of the EU and the USA, in particular, was studied by Lekota and Coetzee [18].

As can be seen from the above-mentioned studies, it is proposed to identify priorities to improve the system of cyber protection of aviation infrastructure, but mainly focused on the subjects of civil aviation activities, paying insufficient attention to the international legal aspects of cybersecurity of civil aviation. In our opinion, it is at the international level that international specialized organizations should propose comprehensive approaches to ensuring cyber security of the civil aviation sector.

In 2013, ICAO, Airports Council International (ACI), Civil Air Navigation Services Organization (CANSO), International Air Transport Association (IATA), and International Coordinating Council of Aerospace Industries Associations (ICCAIA) joined their efforts and created the Industry High Level Group (IHLG), whose task was to implement cooperation on issues of mutual importance, including cyber security. At the international level, it was emphasized that cybersecurity was an issue of high priority for all stakeholders involved in the aviation field [19]. Several measures were proposed, based on agreed policies. However, the work did not stop there, because only the most important areas were outlined at the time, and the planned measures were not comprehensive. It is important not only to form a "set" of objectives for the plan but to view the conceptual vision of cybersecurity as a symbiosis of human capacity, technology, processes, and communications, as well as the necessary regulation for it all at the level of aviation actors, national and supranational levels. This necessitates scientific research to form a holistic vision and develop ways to implement an international cybersecurity strategy for comprehensive civil aviation cyber security.

The purpose of the study is to determine the methodological basis for the development of an international civil aviation cybersecurity strategy, taking into account the existing

experience of strategic planning at the level of international specialized organizations.

3. Research Methods and Methodology

The study of the methodological basis for the development of an international civil aviation cyber security strategy was conducted in four stages.

During the *first stage* of the research, strategic documents and recommendations were analyzed and the main directions of development of strategic cyber planning measures to enhance cyber resistance and security of international aviation infrastructure in the activities of international specialized organizations were systematized, in particular:

International Civil Association Organization (ICAO);

International Air Transport Association (IATA);

International Coordinating Council of Aerospace Industries Associations (ICCAIA);

European Organization for the Safety of Air Navigation (EUROCONTROL)

At the *second stage*, the analysis of the provisions of universal level documents adopted under the aegis of UN and International Telecommunication Union was carried out to identify and systematize the conceptual provisions that constitute a priority for implementation shortly.

Publicly available documents and reports (resolutions and program documents, transcripts of the speeches at the sessions during the meetings of international organizations), used during the first and second stages, are publicly available on the websites of relevant international organizations (ICAO, IATA, ICAIA, EUROCONTROL) for the last 5 years.

During the *third stage*, a comparative analysis of special and general (universal) approaches to the development of international civil aviation cybersecurity strategy is carried out and the differences between them and common methodological bases are clarified. Finally, in the final stage, the identified differences and gaps are summarized and recommendations are formed.

A limitation of the study is that the authors did not have access to documents of intergovernmental organizations that are not intended for free distribution. But this is not a hindrance, because most of the documents reviewed are strategic level and intended for familiarization of the wide audience.

4. Results and Discussion

The analyzed strategic documents and recommendations of the international aviation organizations provide for an expanded list of cyber defense strategies implementation areas. The most structured is Cybersecurity Strategy and Cybersecurity Action Plan ICAO [20; 21].

The Aviation Cybersecurity Strategy bring into line with other cyber-related ICAO initiatives and coordinated with matching safety and security management provisions. The Strategy's aims will be achieved through a series of principles, measures, and actions contained in a Framework built on seven pillars (See Fig 1.):

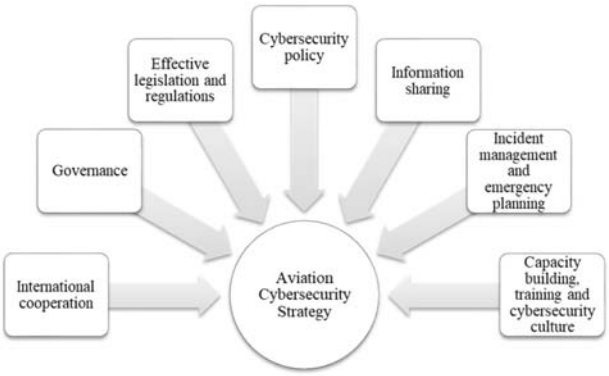

Fig. 1. Aviation Cybersecurity Strategy Framework.

The Cybersecurity Action Plan includes 26 priority activities and 54 detailed activities and tasks to be implemented jointly by the ICAO, member states, and stakeholder organizations. A common feature of this Cybersecurity Strategy with the strategic documents on cybersecurity at the universal level (ITU, Cyber Security Index) [22] is the understanding of the complexity of cybersecurity and the need to develop and implement cyber preparedness programs to improve the effectiveness and capacity of the main components of cybersecurity - human capacity, technology, and necessary processes, including communication and their regulatory support.

ITU, developing a methodology to measure national cyber preparedness, the Cyber Security Index (GCI), offered a clear structure that can serve as a "framework" for cyber strategies and implementation plans in the civil aviation sector.

The GCI main features are a better understanding of countries' commitments to cybersecurity, identifying gaps, encouraging the incorporation of good practices, and providing useful insights for countries to improve their cybersecurity postures.

The GCI results among 194 which was measured in 2020 show overall improvement and strengthening of all five pillars of the cybersecurity agenda (legal measures; technical measures; organizational measures; capacity development measures; cooperation measures) (see Fig 2).

Fig. 2 Global commitments of GCI specific indicators in 2020

In our opinion, unification of approaches based on the ITU Cyber Security Index looks appropriate for international organizations in the civil aviation sphere, primarily for ICAO, which methodologically allows presenting a systemic vision of cyber security regardless of sectoral specifics - be it the civil aviation sector or other critical infrastructure sectors like financial or energy, water or chemical sectors and others.

It is worth further reviewing the measures that have been proposed within ICAO and providing a critical analysis of them in the scientific discussion, based on the proposed paradigm of cyber security comprehensiveness (human capacity, technology, processes and communication, regulatory support).

It is worth noting that the UN Security Council in Resolution 2039 (2016) assessed the role of ICAO as a universal organization to ensure all areas of civil aviation, including the security policy component, noting that it supports and welcomes the work that ICAO does to ensure continuous review and modification of aviation security measures according to the constantly changing nature of global threats, and encourages ICAO within its mandate to continue and increase efforts to ensure compliance with international Of all the threats to civil aviation security, the newest is certainly the rapid spread of cyber technology in aviation, "and the more we rely on computers and information technology, the more we expose ourselves to cyber threats. ICAO also understands this problem and is working with member states to identify vulnerabilities and the most effective countermeasures". [24]

In more detail, the main areas of joint efforts of ICAO member states to improve cyber security in civil aviation were identified in proposals made by Slovakia on behalf of the European Union and its member states, as well as other member states of the European Civil Aviation Conference, and EUROCONTROL and voiced at the 39th session of the ICAO Assembly. In addition to other important aspects, it was proposed to ask ICAO to comprehensively address the issue of cyber-styling in civil aviation [25].

Resolution A39-19, adopted in 2016, is important for the regulation of international cooperation of ICAO member states in addressing the cyber security of civil aviation. During the 39th session of the ICAO Assembly. This document enshrines all the main areas of countering cyber threats, among which special attention is defined concerning the responsibilities of national authorities to combat cyber threats, promoting coordination between member states, and promoting the development and implementation of international standards, strategies, and best practices in the field of civil aviation protection [26]. During this session, a list of possible actions by regulators and stakeholders in the area of cybersecurity was identified at the suggestion of several states [27]. First of all, it was suggested that at the universal level, ICAO should develop a global program to combat cyber threats for all stakeholders. Second, at the state level, it is important to develop a regulatory oversight mechanism by aviation security authorities. In doing so, the regulatory oversight regime should be comprehensive, covering the civil aviation sector and all participants in the civil aviation system, taking into account their interdependence. Finally, at the stakeholder level, each stakeholder needs to develop its own set of actions to protect against cyber threats, especially when it comes to systems that deal with flight safety and aviation security [28], [29].

The recommendations from the 13th Aeronautical Conference (2018), presented by Canada, Austria (on behalf of the EU), EUROCONTROL, Singapore, and supported by Australia and New Zealand, are significant. After discussing aviation as a system of systems (an aviation system evolves from a diversity of digital networks and components interconnected and interdependent in the sense of exchanging digital data and information), the Conference made important recommendations regarding continuous coordination between all important stakeholders, joint activities and coordination among subsystem managers, the need for a working network to mitigate cyber threats and risks to civil aviation systems. This can be expressed in Standards and Recommended Practices (SARPS) in the Annexes to the 1944 Chicago Convention [30].

In our opinion, also noteworthy is the document proposed by the United States for consideration by the 40th ICAO Assembly that addresses cybersecurity and resilience management as a multidisciplinary issue that touches on almost all aspects of global aviation. Today, the leadership on cyberspace issues is divided between the Air Transport Bureau (ATB) (cybersecurity issue) and the Air Navigation Bureau (ANB) (cyber resilience issue). In this situation, according to American experts, the optimal organizational model would be the creation of a technical committee on cybersecurity and resilience [31]. That is, it is a matter of unifying rules to avoid overlapping functions, copying, and vice versa gaps due to potential competition between functions, where there may be an excessive expenditure of

resources in one task and a lack of attention and resources on others.

The next step to enhance international cooperation in combating cyber threats and civil aviation was the adoption in 2019. During the 40th ICAO Assembly, several documents, including Resolution A40-10, "Addressing Cybersecurity in Civil Aviation." This document defines a detailed, expanded plan for ICAO member states to address cyber threats to civil aviation, focusing in particular on cybersecurity strategy, assessment and anticipation of threats, risks to flights and critical civil aviation systems, and the serious consequences that such incidents can lead to. During the Assembly, the role of national authorities and stakeholders and the importance of cooperation in developing an ICAO cybersecurity program according to a unified, comprehensive, and functional approach that includes the areas of air navigation, communications, surveillance, aircraft operations, airworthiness, and other relevant disciplines were emphasized [32]. In addition, Resolution A40-11 provides specific practical steps to ensure civil aviation cybersecurity [33], which are extremely important, but without a detailed implementation plan, methodological assistance, and consideration of national specifics (limited resources, qualified personnel), their implementation may not be as effective as planned. The lack of a programmatic approach, in our opinion, may become a key obstacle to the effective implementation of these measures at the national level.

As we mentioned above, one of the main coordination documents of ICAO in this area is the current Cybersecurity Action Plan (CyAP). The key priorities of the Plan are: 1) creating a cybersecurity culture; 2) ensuring that the civil aviation system is cyber secure; 3) ensuring civil aviation is self-reinforcing by adopting an "embedded security" (by design, by default) approach 4) aligning with other ICAO cybersecurity initiatives, coordinating with and utilizing regulations on flight safety management and aviation security. The Plan defines the main cybersecurity strategies as 1) international cooperation; 2) governance; 3) applicable laws and regulations; 4) cybersecurity policy; 5) information sharing; 6) incident management and contingency planning; and 7) cybersecurity capacity building, training, and culture [32].

From the above list of directions, it can be seen that some of them are very similar in the content of the activities that are covered. For example, directions three (regulatory) and four (cyber security policy) use the same toolkit - regulatory. The fifth (information sharing) and sixth (incident management) are different levels of coordination and management of the same process of responding to security threats and incidents, which includes information sharing both in normal mode and in crisis situations. So, the third and fourth, as well as the fifth and sixth directions can be methodologically combined. As a result of such integration, we come to a model, similar to the ITU Cyber Security Index, on which an international strategy on comprehensive cyber security of civil aviation and a roadmap for its implementation can be built.

5. Conclusions

Based on the above, it is reasonable to propose the structure of an international strategy for the comprehensive cyber security of civil aviation in five key areas: (1) legal; (2) technical; (3) organizational; (4) capacity development; (5) cooperation. These directions propose to cover such sub-directions and specific tasks:

1. The legal direction focuses on the maturity of the legislative and regulatory environment, which defines the basic requirements for cybersecurity of critical aviation infrastructure, the tasks and powers of aviation agencies, minimum cybersecurity requirements for civil aviation entities, implementation of cybersecurity measures, requirements for information security audits at aviation infrastructure facilities.
2. The technical direction includes the development of an international network of specialized Computer Security Incident Response Teams/Security Control Centers (CSIRTs/SOCs) for the civil aviation sector, the implementation of international standards and regulations, the identification of technical capabilities to ensure security and resilience, management and response to cyber-attacks.
3. The organizational pillar covers strategic/policy documents and mechanisms and structures for the response, prevention, and recovery from cyber-attacks. This level also covers national-level requirements for resilience plans, readiness audits, and cyber risk assessments of aviation activities, air navigation infrastructure, and the like.
4. Capacity development refers to cybersecurity awareness activities, certification of cybersecurity professionals, availability of cybersecurity training programs for civil aviation professionals, research activities (malware analysis, cryptography research, and other research), and stimulating government efforts to encourage cybersecurity capacity building among both aviation actors and other stakeholders.
5. Cooperation covers participation in international cooperation, membership in international organizations, public-private partnership practices, cooperation among stakeholders, and implementation of best practices on cyber security in the civil aviation sector.

The practical value of the proposed approach is that it can be used not only to develop an international strategy for cyber security in civil aviation, but also to develop a roadmap for strategy implementation at the national level by governments of states. It is also important to periodically revise approaches and adapt them to new challenges in the field of cyber security, which is what the proposed methodological framework will allow.

Prospects for further research include the development of unified indicators at the international level to assess the implementation of the provisions planned in the strategies.

References

[1] A/RES/54/49. UNGA Resolution Developments in the field of information and telecommunications in the context of international security (1999). Available at: https://undocs.org/A/RES/54/49.

[2] Nashynets-Naumova, A. (2013). Pravovoye regulirovaniye informatsiynoi bezpeki v tsivil'niy aviatsii: mezhdunarodno-pravoviy aspekt. *Vísnik NTTU KPI. Politologiya. Sotsiologiya. Pravo. Reviews*, 3 (19), 155-160. Available at: http://nbuv.gov.ua/UJRN/VKPI_soc_2013_3_28.

[3] Goncharova, N.A. (2018). Regulirovaniye kiberbezopasnosti grazhdanskoy aviatsii: vnedreniye modernizatsii NEXTGEN v Rossii i USA. *Zhurnal «Biznes. Obshchestvo. Vlast'»*. July 2018. № 2 (28). P. 175-205. Available at: https://www.hse.ru/data/2018/08/18//.pdf

[4] Klenka, M. (2021) Aviation cyber security: legal aspects of cyber threats. *J Transp Secur*. https://doi.org/10.1007/s12198-021-00232-8

[5] Abeyratne, R. (2011) Cyber terrorism and aviation—national and international responses. *J Transp Secur* 4, 337–349. https://doi.org/10.1007/s12198-011-0074-3

[6] S. J. da Silva and J. M. R. Silva. (2021). Cyber Risks In The Aviation Ecosystem: An Approach Through A Trust Framework. *Integrated Communications Navigation and Surveillance Conference (ICNS)*, 2021, pp. 1-12, doi: 10.1109/ICNS52807.2021.9441596.

[7] EUROCONTROL (2019). Aviation Intelligence Unit. Think Paper #3—August 2019. Cyber Security in aviation. Available at: https://www.eurocontrol.int/sites/default/files/2020-01/eurocontrol-think-paper-3-cybersecurity-aviation.pdf.

[8] Abeyratne, R. (2011) Cyber terrorism and aviation—national and international responses. *J Transp Secur* 4, 337–349. https://doi.org/10.1007/s12198-011-0074-3

[9] F. Alrefaei, A. Alzahrani, H. Song, M. Zohdy and S. Alrefaei (2021). Cyber Physical Systems, a New Challenge and Security Issue for the Aviation. *2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. pp. 1-5, doi: 10.1109/IEMTRONICS52119.2021.9422483.

[10] Nickolaos Koroniotis, Nour Moustafa, Francesco Schiliro, Praveen Gauravaram, Helge Janicke (2020). A Holistic Review of Cybersecurity and Reliability Perspectives in Smart Airports. *Access IEEE*. vol. 8. pp. 209802-209834. doi: 10.1109/ACCESS.2020.3036728.

[11] J. Pollack and P. Ranganathan (2018). Aviation Navigation Systems Security: ADS-B GPS IFF. *Proceedings of the International Conference on Security and Management (SAM)*. pp. 129–135.

[12] Lykou G., Iakovakis G., Gritzalis D. (2019) Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management. In: Gritzalis D., Theocharidou M., Stergiopoulos G. (eds) Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-030-00024-0_13

[13] Goncharova, N.A. (2018). Regulirovaniye kiberbezopasnosti grazhdanskoy aviatsii: vnedreniye modernizatsii NEXTGEN v Rossii i USA. *Zhurnal «Biznes. Obshchestvo. Vlast'»*. July 2018. № 2 (28). P. 175-205. Available at: https://www.hse.ru/data/2018/08/18//.pdf

[14] R. Abeyratne (2016). Aviation Cyber Security: A Constructive Look at the Work of ICAO. *41 Air & Space Law* 25, 26–29. Available at: https://www.kluwerlawonline.com/abstract.php?area=Journals&id=AILA2016003

[15] D. Jeyakodi (2015), Cyber Security in Civil Aviation, *Aviation & Space J.*, no. 4, Oct.–Dec. Jeyakodi 2015, 11 – 17.

[16] B. Lim (2014), Aviation Security: Emerging Threats from Cyber Security in Aviation – Challenges and Mitigations, *J. Aviation MGMT*. 83. Available at: http://www.saa.com.sg/saaWeb2011/export/sites/saa/en/Publication/downloads/EmergingThreats_CyberSecurityinAviation_ChallengesandMitigations.pdf

[17] M. Pierides, et al. (2015), Cybersecurity and the Aviation Sector: Recent Incidents Highlight Unique Risks, *Pillsbury Law*, Available at: https://www.pillsburylaw.com/images/content/1/1/v2/1196/AlertAug2015GlobalSourcingCybersecurityandTheAviationSector.pdf.

[18] Lekota, Faith; Coetzee, Marijke. (2021). Aviation Sector Computer Security Incident Response Teams: Guidelines and Best Practice. *European Conference on Cyber Warfare and Security. Reading,* (Jun 2021). DOI:10.34190/EWS.21.028

[19] Petrova, R.Ye. (2020) Pravovyye aspekty bezopasnosti poletov v usloviyakh kiberugroz: na primere grazhdanskoy aviatsii. *Monitoring pravoprimeneniya*. № 1 (34). p. 56 – 60. DOI: 10.21681/2226-0692-2020-1-56-60

[20] ICAO (2019). Aviation Cybersecurity Strategy. Available at: https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf.

[21] ICAO (2020). Cybersecurity Action Plan (CyAP). Available at https://www.icao.int/cybersecurity/Pages/Cybersecurity-Action-Plan.aspx.

[22] ITU. Global Cybersecurity Index. Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[23] Resolution 2309 (2016). Adopted by the UN Security Council at its 7775th meeting, on 22 September 2016. Available at: https://undocs.org/en/S/RES/2309(2016)

[24] S/PV.8057 (2017). Threats to international peace and security caused by terrorist acts, Aviation security. UN Security Council, 8057th meeting 27 September 2017, New York. Available at: https://undocs.org/en/S/PV.8057

[25] Bernard Lim (2016). Civil Aviation Cybersecurity: Possible Actions by Regulators and Stakeholders. Available at: https://www.ecac-ceac.org/images/news/ecac-news/ECAC-News_56_Aviation_in_Asia-Pacific.pdf

[26] ICAO (2016). A39-WP/236. Coordinating Cybersecurity Work. Available at: https://www.icao.int/Meetings/a39/Documents/WP/wp_236_rev1_en.pdf

[27] ICAO (2016). A39-WP/99. Cyber Resilience in Civil Aviation. Available at: https://www.icao.int/Meetings/a39/Documents/WP/wp_099_en.pdf

[28] ICAO (2016). A 39/19. Addressing Cybersecurity in Civil Aviation. Assembly – 39th session. Montréal, 27

September—6 October 2016. p. 99-101. Available at: https://www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf

[29] ICAO (2016). A39-WP/175. Civil Aviation Cybersecurity: Possible Actions by Regulators and Stakeholders. Assembly — 39th session. Montréal, 27 September—6 October 2016. Available at: https://www.icao.int/Meetings/a39/Documents/WP/wp_175_en.pdf

[30] ICAO (2018). AN-Conf/13-WP/270. System-of-Systems Notion of Cybersecurity in Aviation. Montréal, 9-19 October 2018. Available at: https://www.icao.int/Meetings/anconf13/Documents/WP/wp_270_en.pdf

[31] ICAO (2019) A-40-WP/427 Proposal for ICAO Governance of Cybersecurity and Resilience. Assembly — 40th Session. Available at: https://www.icao.int/Meetings/a40/Documents/WP/wp_427_en.pdf

[32] ICAO (2019). A40-10. Addressing Cybersecurity in Civil Aviation. Assembly – 40th session. Available at: https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf

[33] ICAO (2019). A40-11. Consolidated statement on continuing ICAO policies related to aviation security. Assembly – 40th session. Available at:https://www.icao.int/Meetings/a40/Documents/Resolutions/a40_res_prov_en.pdf