ESJ Social Sciences Peer-reviewed

Ethical Issues of Generative AI in the Aviation Cybersecurity Environment

Malgorzata Zmigrodzka, PhD
Polish Air Force University in Deblin, Poland

Doi:10.19044/esj.2025.v21n25p39

Submitted: 25 June 2025
Accepted: 05 September 2025
Published: 30 September 2025

Cite As:
Zmigrodzka, M. (2025). *Ethical Issues of Generative AI in the Aviation Cybersecurity Environment.* European Scientific Journal, ESJ, 21 (25), 39.
https://doi.org/10.19044/esj.2025.v21n25p39

Abstract

The present study aims to analyze the ethical issues related to the use of generative artificial intelligence in aviation, with a particular focus on cybersecurity aspects. Therefore, all existing ethical concerns regarding bias, misinformation, fraud, privacy, and copyright infringement on the internet apply equally to content created by generative artificial intelligence. These concerns underscore the well-documented issues about the bias of internet search engine algorithms. Numerous parties have contended that ethical considerations should have been a factor in the development of this technology.

This article discusses the results of a survey conducted among students of the Polish Air Force Academy, which addresses key issues related to regulation, training, and awareness-raising regarding the ethical use of artificial intelligence. A mixed-methods approach was utilized in the present study. Quantitative data were collected via an online survey (N = 57, F = 27, M = 30) conducted between September and October 2024. Furthermore, a total of 15 semi-structured anonymous interviews were conducted with experts in cybersecurity and AI ethics to obtain qualitative information. The interviews were conducted with aviation specialists, cybersecurity analysts, and AI ethics researchers who had between five and 20 years of experience. The aviation sector was selected as the subject of the study due to its high sensitivity to technological risk, its reliance on secure systems, and the critical importance of public trust in automated and AI-assisted systems. In Poland, there is only one university that specializes in aviation and accepts both military and

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

civilian students. This research will make a substantial contribution to enhancing aviation safety in the future through the implementation of a robust management framework based on comprehensive knowledge. This research is of particular pertinence in the context of the ongoing war in Ukraine and in Poland's neighborhood.

Keywords: Security, ethics, causal networks, ChatGPT, generative AI, agility

Introduction

The advent of generative AI technologies has precipitated a paradigm shift within the domain of cybersecurity. While these technologies undoubtedly enhance automation, they also introduce risks such as biased results, misinformation, and privacy issues. The present paper puts forward a series of empirical, research-based ethical issues to address these challenges. The moral and regulatory considerations of AI have been a subject of deliberation among legislators, governments, and technologists worldwide for an extended period. After these deliberations, the High-Level Expert Group on AI promulgated the Ethical Guidelines for Trustworthy Artificial Intelligence in 2019. On 14 June 2023, the European Parliament passed the world's first piece of legislation designed to regulate the use of artificial intelligence: the AI Act. The provisions of the AI Act apply to all companies that place AI systems on the market or make them available for use, irrespective of their geographical location. The AI Act delineates four categories of risk associated with the utilization of AI-based systems:

Low risk: This category encompasses systems that are deemed to pose a minimal risk. This is considered to be a medium-risk scenario. This category encompasses chatbots that have garnered significant popularity in recent months, including ChatGPT. It is important to note that the present situation is of a high-risk nature. This category encompasses technologies that have the potential to impact users' safety and fundamental rights.

The potential repercussions of this decision are such that they cannot be considered acceptable. This category encompasses systems that present a significant safety risk. Examples of such systems include those designed for social scoring. The AI Act proscribes a range of AI practices deemed unacceptable in each category. In this article, the author focuses on the issues in the field of aviation. It is vital to acknowledge the strategic relevance of the aviation sector to national security, international logistics, and critical infrastructure. Consequently, this sector is particularly vulnerable to the risks and challenges posed by generative AI technologies. The utilization of services and systems founded upon artificial intelligence algorithms empowers smart airports to enhance reliability, efficiency, and control. This

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

augmentation is facilitated through the implementation of real-time monitoring and analysis (Żmigrodzka, 2024).

It is therefore evident that the regulation and cybersecurity resilience of the system are of paramount importance.

Methods

The purpose of this study is to analyze ethical issues related to the use of generative artificial intelligence (AI) in the aviation sector, with a particular focus on cybersecurity.

The author's goal was to identify the main ethical and cybersecurity risks arising from the implementation of generative artificial intelligence in the aviation sector. In addition, the results of the study concerning the perception of risks associated with artificial intelligence by students of both aviation and cybersecurity are of particular interest.

A mixed-methods approach was used in this study. Quantitative data were collected via an online survey (N = 57, F = 27, M = 30) conducted between September and October 2024. The data were analyzed using thematic categorization and visualization techniques. The study was conducted at the Air Force Academy, examining the number of students enrolled in undergraduate and graduate programs in aviation and cybersecurity. The target group for the study was students aged 20–26. There is only one aviation academy in Poland that offers aviation training for both military and civilian students. The main element of the study was to assess their knowledge and experience in the use of artificial intelligence. Participants were asked to answer fifteen questions about cybersecurity, generative artificial intelligence, and ethics. In addition, a total of 15 semi-structured anonymous interviews were conducted with experts in the field of cybersecurity and artificial intelligence ethics to obtain qualitative information. The interviews involved aviation specialists, cybersecurity analysts, and researchers in AI ethics with between five and 20 years of experience. The same survey questions were used to compare the approach of the younger generation with that of the more experienced audience. In addition, master's students from an aviation academy were included in the study. The interview questions focused on identifying ethical risks, regulatory gaps, and the responsibilities of humans and artificial intelligence.

The research questions are as follows:

The main research question:

What ethical and cyber threats arise from the use of generative artificial intelligence in the aviation sector?

Detailed research questions further develop the research problem:

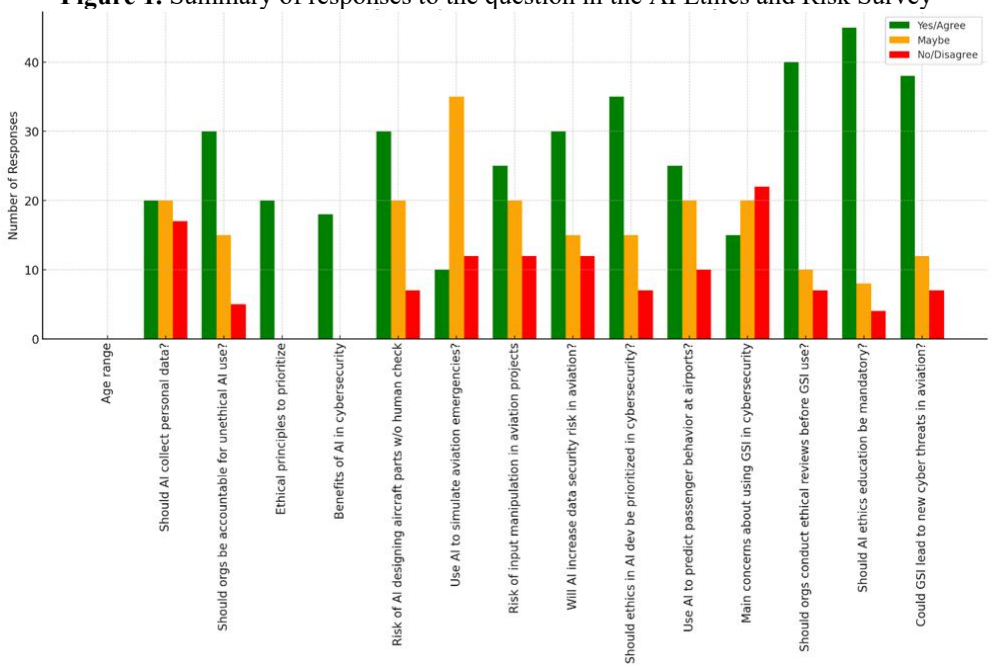
 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

1. Could making ethical education mandatory for AI developers and users reduce the risk of abuse in the aviation environment?
2. How can a coherent ethical framework for the use of generative AI in high-risk sectors such as aviation be developed?
3. What regulatory gaps and deficiencies in ethical oversight need to be addressed for generative AI to be implemented in the aviation environment?
4. What are the attitudes of future aviation professionals towards the ethics of AI use in safety-critical situations?
5. In what ways might generative AI affect the safety of aviation operations, including component design and technical diagnostics?

Results

This is a summary and visual analysis of a study on artificial intelligence, ethics, and cybersecurity. The bar chart shows how 57 students from the Polish Air Force University responded to 15 key questions, and illustrates how opinions are distributed in terms of "Yes/Agree", "Maybe", and "No/Disagree". Semi-structured interviews revealed concerns about accountability gaps in AI-driven aviation systems, particularly in high-risk areas such as flight control, component design, and maintenance diagnostics. Experts emphasized the need for human oversight, regulatory harmonization, and the ethical training of AI developers in aviation.

Figure 1. Summary of responses to the question in the AI Ethics and Risk Survey

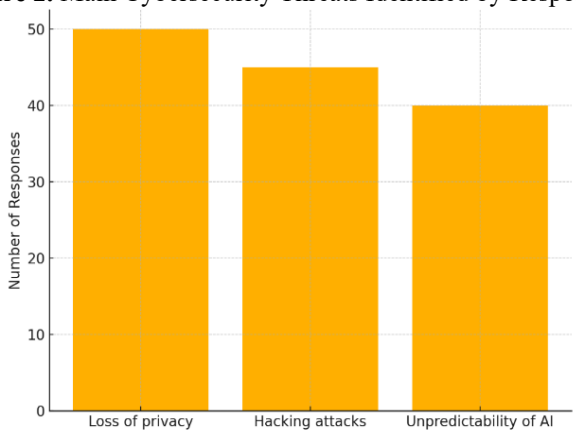


Source: Own research

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

The survey results revealed significant insights into perceptions of AI risks and ethical concerns in cybersecurity. Participants identified the following key cybersecurity threats: loss of privacy, hacking attacks, and the unpredictability of AI behaviour. Participants overwhelmingly agreed that organisations developing AI should conduct mandatory ethics reviews and that AI ethics education should be made mandatory. Experts emphasised the need for regulatory harmonisation and human oversight, highlighting accountability gaps in AI systems used in aviation.

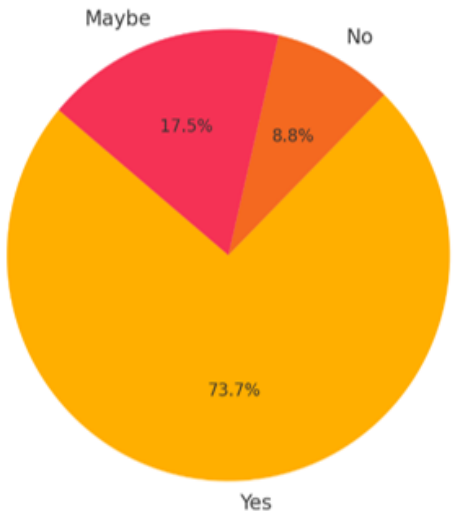
Figure 2. Main Cybersecurity Threats Identified by Respondents.



Source: Own research

Participants overwhelmingly (over 73%) agreed that organizations developing AI should conduct mandatory ethics reviews.

Figure 3. Should Organizations Conduct AI Ethics Reviews?

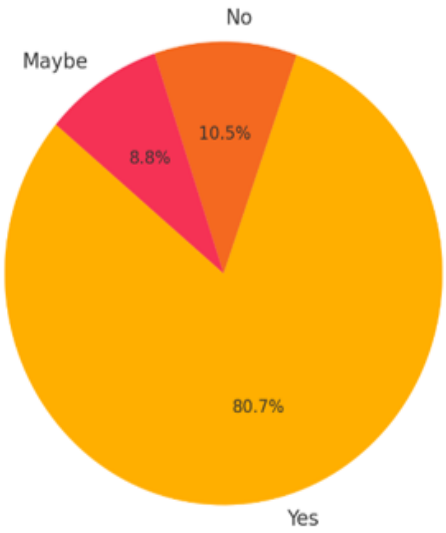


Source: Own research

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Similarly, the majority (over 80%) supported making AI ethics education mandatory for all employees handling AI systems.

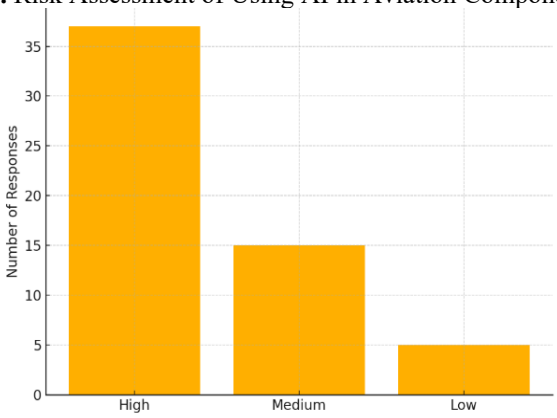
Figure 4. Should AI Ethics Education be Mandatory?



Source: Own research

The majority of respondents assessed the risks of using AI for designing aviation components as high, highlighting the critical need for human oversight.

Figure 5. Risk Assessment of Using AI in Aviation Component Design.



Source: Own research

Figure 5 shows that more participants consider the use of AI in aviation component design to be high-risk, aligning with expert concerns about reliability, explainability, and system resilience. This underscores the urgent

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

need for sector-specific regulations that can guide responsible AI integration in aviation.

A series of interviews was conducted with aviation experts, the results of which indicated a degree of concern regarding the utilization of artificial intelligence within the aviation industry. It is posited that the fundamental components of cybersecurity can be distilled into three elements. It is imperative to acknowledge that systems and organizations possess vulnerabilities that, if exploited, have the potential to introduce risks that could compromise their operational integrity. A threat, such as malware, is a potential vulnerability that can be exploited to cause harm to a system or organization. Defensive measures, incorporating security controls and countermeasures, are employed to mitigate identified risks. The advent of artificial intelligence is poised to exert a profound influence on all three elements. The utilization of artificial intelligence (AI) within a system has been demonstrated to enhance its efficacy. However, it should be noted that this integration may simultaneously give rise to new vulnerabilities to cyberattacks. To address these new vulnerabilities, it is essential to gain a more profound understanding of them and to define specific security controls (technical or organizational) for them. In the contemporary context, malware has a propensity to mutate, that is to say, it adapts its behavior to prevailing conditions. The inevitable emergence of AI-based attacks necessitates the identification of appropriate countermeasures, especially in the context of disinformation and terrorist threats. Emotional intelligence is a recently identified competency of significant importance. These novel competencies underscore the emerging psychological challenges confronting aviation professionals in their handling of. It is evident that novel supporting measures and activities must be developed and implemented to address the challenges posed by AI.

Discussion

Analysis of Cybersecurity Gaps in Aviation Organizations

Findings from the conducted survey and interviews provide additional insights into the cybersecurity gaps and ethical concerns highlighted above.

Generative AI introduces cybersecurity gaps, including privacy violations, bias amplification, disinformation threats, operational fraud, and regulatory deficiencies. Proposed solutions include restricted data access, model transparency, employee training, audits, and international regulatory standards.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

AI ethics in the context of aviation

In the field of ethics, it is very important for stakeholders to address the problems indicated in the survey, acting to change perceptions of the research issue:

- Collaboration of industry/research/ethics working groups.
- Expert working groups.
- Discussion between traditional safety development experts and AI software developers.

The proposal after the survey made in the aviation environment and working group was very consistent with EASA suggestions on the importance of promoting training activities, competence development initiatives, and knowledge and information sharing, and the importance of the certification process for AI-based systems, thus ensuring their reliability and safety. The EASA, as the authority of safety and security in aviation, must assess the evolution of AI and its impacts. They must alert politicians and stakeholders, show them the possibilities and risks, but should never regulate on its own initiative, or even suggest regulations on ethics. In a democracy, this is the business of the elected assemblies. EASA should ensure that only highly qualified AI professionals are involved before implementing such systems. There is a need for an independent security council that will oversee, vet, and regulate EASA and FAA in relation to AI.

Documented Incidents in Aviation Cybersecurity

The need for research, which was conducted in the article, confirms several real-world cases. There is an urgency to reinforce cybersecurity and ethical oversight in aviation technologies. In 2015, security researcher Chris Roberts claimed he accessed aircraft onboard systems via the in-flight entertainment system (IFE), potentially influencing flight control. Although controversial, his claims highlighted the risks of interconnecting IFE and flight systems. Also in 2015, LOT Polish Airlines experienced a cyberattack that disrupted its ground computer systems at Warsaw Chopin Airport. The DDoS attack led to flight cancellations and exposed vulnerabilities in airline IT infrastructure. In 2018, British Airways was targeted in a malware attack that affected its website and mobile app. Personal and financial data of nearly 500,000 passengers were stolen, resulting in major reputational and financial damage. In 2021, Eurocontrol was targeted by pro-Russian hackers using a DDoS attack aimed at disrupting European air traffic operations.

In 2023, cyberattacks on GNSS (Global Navigation Satellite Systems) escalated, with GPS signal interference reported in the Middle East, affecting both commercial and military flights.

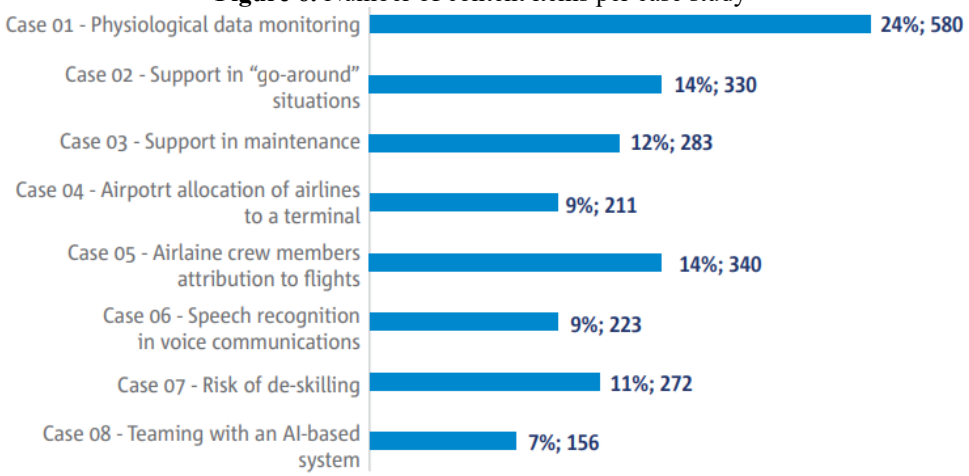
 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Ethics-based assessment for AI-based systems applied in aviation — summary of the results

EASA has been working on ethical issues for AI in aviation, with 231 respondents, 171 expressed a 'non-acceptance' opinion for at least one of the eight scenario cases. To understand the reasons why AI-based systems were seen as ethically unacceptable, 2,395 content items in total were analysed and categorised in this study.

The distribution of the content items for the eight scenario cases is as follows:

Figure 6. Number of content items per case study



Source: Aviation Professionals Survey Results 2024/2025, https://www.easa.europa.eu/en/document-library/general-publications/ethics-artificial-intelligence-aviation#group-easa-downloads (28.08.2025)

The motives behind the non-acceptance of AI-based systems for the eight cases considered show that aviation professionals have ethical concerns about the AI-based system itself (30 %), about the consequent negative impact on humans when using such systems (28 %), about how their data is used by the technology (11 %), and about AI-based systems putting aviation safety at risk (6 %). The results of the present study demonstrate that, in the context of safeguarding ethical values, aviation professionals anticipate that the primary aviation industry will guarantee that AI-based systems are transparent, explainable, reliable, and adhere to the established standards. It is imperative that, even in circumstances where artificial intelligence is employed as a facilitator for more sophisticated automation, human beings should continue to exercise autonomy in decision-making and system oversight. Furthermore, they must be empowered to preserve their autonomy. Users must not experience psychological discomfort and can engage with an AI-based system as if it were merely a machine.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Literature review

Recent literature highlights the dual potential and risks of deploying generative AI in cybersecurity.

Ligot (2024) emphasises the importance of structured AI governance, as set out in the 4E Framework: Education, Engineering, Enforcement, and Ethics. His work highlights critical generative AI challenges such as biased training data, prompt manipulation, and content misuse, and outlines the distinct roles of stakeholders such as builders, users, and trainers in the development of responsible AI.

Meanwhile, Wang (2024) explores the emerging threats posed by generative AI, including data privacy violations, AI fraud, and adversarial attacks. He advocates for proactive countermeasures such as improved standards, public education, and technical safeguards to prevent misuse and ensure robust cybersecurity defences.

Kritika (2024) discusses the application of generative AI for anomaly detection, synthetic data generation, and automated incident response in cybersecurity. While acknowledging its potential to strengthen security operations, she also raises concerns about risks related to adversarial manipulation, model extraction, and deepfakes. Her work emphasises the importance of explainability, adversarial robustness, and ethical design in AI-powered security systems.

The studies by Gupta et al. (2023) focus on the offensive capabilities enabled by generative AI, including automated spear-phishing, identity spoofing, and the creation of adaptive malware, underlining how AI is lowering the barrier for cybercriminal activity. Kam et al. (2024) highlight significant regulatory and institutional gaps in addressing these threats, particularly noting the absence of sector-specific AI risk governance frameworks in aviation.

Rodgers et al. (2023) address the socio-technical implications of AI deployment in critical infrastructure, emphasizing the importance of stakeholder trust, transparency, and explainable AI models to support human oversight. In contrast, Nah et al. (2023) explore the operational integration of AI in security systems, identifying challenges related to system interoperability, false positives in anomaly detection, and reliance on synthetic data in training models.

Singh et al. (2024) provide insights into ethical frameworks for AI-powered cybersecurity, proposing principles for fairness, responsibility, and continuous monitoring, while Kushwaha (2024) argues for embedding human-centered values in cybersecurity policies and training protocols to mitigate the unintended consequences of autonomous AI systems.

Together, these studies reinforce the necessity for a multidisciplinary, policy-informed, and ethically grounded approach to the governance and

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

application of generative AI, particularly within high-risk sectors such as aviation, where cyberattacks can have cascading effects on safety, logistics, and international mobility.

Recent research by Ferrag et al. (2025) provides a thorough examination of the cybersecurity landscape as influenced by generative AI. The study outlines various vulnerabilities, such as prompt injection, data leakage, adversarial inputs, and model hallucinations, which emerge from the use of large language models (LLMs) in cybersecurity systems. The authors also propose mitigation techniques, such as reinforcement learning with human feedback (RLHF), retrieval-augmented generation (RAG), and adversarial training. These methods are presented as essential for developing secure and responsible AI systems in critical infrastructure sectors, such as aviation.

Similarly, Ibrar (2025) frames generative AI as a double-edged sword, emphasizing its use by both malicious actors and cybersecurity professionals. His work highlights the risks of automating phishing, malware generation, and synthetic media for disinformation, while recognizing GenAI's potential to support automated threat detection, anomaly monitoring, and real-time response mechanisms. Ibrar, therefore, advocates placing greater emphasis on governance, model transparency, and human oversight in order to balance these opposing dynamics within cybersecurity environments.

Conclusions

This study aimed to analyze ethical issues related to the use of generative artificial intelligence in the aviation environment, with a particular focus on cybersecurity. This aim was successfully achieved. The use of a mixed research method provided important insights into the technical and ethical aspects of implementing generative artificial intelligence.

The study provided concrete, evidence-based answers to basic and detailed research questions:

1. The following key ethical and cyber risks were identified: data privacy violations, bias in AI models, lack of transparency, unpredictable AI behavior, and insufficient human oversight.
2. The impact of generative AI on aviation safety is a concern, as it may pose risks in critical areas such as component design, flight planning, and diagnostics. This requires the implementation of human-operated mechanisms and explainable AI systems.
3. Most students were in favor of introducing mandatory ethics education, emphasizing its key role in preventing abuse and promoting the responsible implementation of AI.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

4. Experts identified regulatory fragmentation and the lack of enforceable ethical standards as significant gaps in oversight, particularly in a cross-border context.
5. The results of both the expert opinions and student responses indicate that the implementation of mandatory ethics training could significantly reduce the risk of unethical AI implementation in the aviation sector.

The relationship between generative AI, cybersecurity, and aviation safety requires the urgent development of a coherent ethical framework, supported by international regulatory cooperation. The integration of generative AI with cybersecurity requires the establishment of a scalable ethical framework that prioritizes transparency, accountability, and human oversight. It is recommended that future research be international in scope and address the evolving risks of AI in critical sectors such as aviation.

It is clear that authorities such as the Federal Aviation Administration (FAA) and the European Union Aviation Safety Agency (EASA) are conducting ongoing assessments and taking action to ensure the safety of aviation systems.

The incidents mentioned above highlight the critical need for an ethical framework and human-centered oversight when implementing artificial intelligence and other digital technologies in aviation.

Cyberspace is becoming an increasingly important area in the context of aviation safety. Cyber threats can cause serious disruptions to aviation, air traffic control systems, and passenger safety. To address these challenges, corrective action is needed by both aviation institutions and regulatory bodies. This can be achieved through a multi-faceted approach, including raising awareness of threats, conducting risk assessments, implementing security standards, applying appropriate technical safeguards, monitoring and responding to incidents, securing suppliers, planning for business continuity, and conducting regular audits and updates.

However, implementing effective countermeasures requires ongoing commitment to interdisciplinary collaboration and continuous monitoring, as well as the ability to adapt to the changing cybersecurity environment. It is essential to recognize that the continued reliability and safety of aviation as a mode of transport in the digital age can only be ensured through the implementation of an integrated, collaborative approach. The convergence of generative artificial intelligence, cybersecurity, and aviation safety requires the rapid formulation of a coherent ethical framework, supported by international regulatory cooperation. Failure to act in this area could expose aviation systems to a range of unprecedented digital threats.

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

Conflict of Interest: The author reported no conflict of interest.

Data Availability: All data are included in the content of the paper.

Funding Statement: The author did not obtain any funding for this research.

References:

1. Aviation Professionals Survey Results 2024/2025, https://www.easa.europa.eu/en/document-library/general-publications/ethics-artificial-intelligence-aviation#group-easa-downloads (28.08.2025)
2. Ethics guidelines for trustworthy AI, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (25.08.2025)
3. EU AI Act: first regulation on artificial intelligence, https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence (25.08.2025)
4. EASA, https://www.easa.europa.eu/en (25.08.2025)
5. FAA, https://www.faa.gov/ (25.08.2025)
6. Ferrag, M. A., Alwahedi, F., Battah, A., Cherif, B., Mechri, A., Tihanyi, N., Bisztray, T., & Debbah, M. (2025). *Generative AI in cybersecurity: A comprehensive review of LLM applications and vulnerabilities*. *Internet of Things and Cyber-Physical Systems*, 5, 1–46. https://doi.org/10.1016/j.iotcps.2025.01.001
7. Gupta, M., Akiri, C., Aryal, K., Parker, E., & Praharaj, L. (2023). From ChatGPT to Threatt: Impact of Generative AI in Cybersecurity and Privacy. IEEE Access, 11, 80218–80237, https://doi.org/10.1109/ACCESS.2023.3300381
8. Ibrar W., Mahmood D., Sami Al-Shamayleh A., Ahmed G., Alharthi S.Z., Akhunzada A. (2025). Generative AI: a double-edged sword in the cyber threat landscape. Applied Intelligence, https://doi.org/10.1007/s10462-025-11285-9.
9. Kam, H.-J., Zhong, C., Johnston, A. C. (2024). The impacts of generative AI on the cybersecurity landscape. Thirty-Second European Conference on Information Systems (ECIS 2024), Paphos, Cyprus, https://doi.org/10.30560/ijas.v8n2p1
10. Kritika, S. (2024). Generative AI for Cybersecurity: An Introduction. Cybersecurity Review, 11(3), 205–221, DOI: 10.4018/979-8-3693-8557-9.ch009
11. Kushwaha, M. P. (2024). The Ethical Dilemmas of AI in Cybersecurity. ISC2 Insights,

 ISSN: 1857-7881 (Print) e - ISSN 1857-7431

https://www.isc2.org/Insights/2024/01/The-Ethical-Dilemmas-of-AI-in-Cybersecurity

12. Ligot D.V., AI Governance: A Framework for Responsible AI Development (May 5, 2024). Available at SSRN: https://ssrn.com/abstract=4817726 or http://dx.doi.org/10.2139/ssrn.4817726
13. Nah, F. F.-H., Zheng, R., Cai, J., Siau, K., & Chen, L. (2023). Generative AI and ChatGPT: Applications, challenges, and AI-human collaboration. Journal of Information Technology Case and Application Research, 25(3), 277–304. https://doi.org/10.1080/15228053.2023.2233814
14. Raman, R., Calyam, P., & Achuthan, K. (2024). ChatGPT or Bard: Who is a better Certified Ethical Hacker? Computers & Security, 140, 103804. https://doi.org/10.1016/j.cose.2024.103804
15. Rodgers, W., Murray, J. M., Stefanidis, A., Degbey, W. Y., & Tarba, S. Y. (2023). An artificial intelligence algorithmic approach to ethical decision-making in human resource management processes. Human Resource Management Review, 33, 100925. https://doi.org/10.1016/j.hrmr.2022.100925
16. Singh, S. P., Tyagi, R., & Mishra, S. (2024). AI-Powered Cybersecurity: Balancing Efficiency and Ethical Considerations. In National Conference on Advancement of Information Technology (NCAIT-2024), Jaipur, India, https://www.researchgate.net/publication/384474301_AI-Powered_Cybersecurity_Balancing_Efficiency_and_Ethical_Considerations
17. Wang, M. (2024), Generative AI: A New Challenge for Cybersecurity. *Journal of Computer Science and Technology Studies*, *6*(2), 13-18, https://doi.org/10.32996/jcsts.2024.6.2.3
18. Żmigrodzka, M. (2023). Impact of new technologies on developing aviation safety training. Safety & Defense, 9(2), https://doi.org/10.37105/sd.207
19. Żmigrodzka, M. (2024). Sztuczna inteligencja a bezpieczeństwo zarządzania operacjami lotniskowymi. Rocznik Bezpieczeństwa Morskiego, XVIII(null), 777-794, https://doi.org/10.5604/01.3001.0054.8329.