

Civil Aviation Cybersecurity in Indonesia: Legal Compliance, Regulatory Gaps, and Reform in Light of ICAO Standards

Adya Paramita Prabandari ^a,  
Ramalina Ranaivo Mikea Manitra ^{b c} 

^a Faculty of Law, Universitas Diponegoro, Semarang, Indonesia

^b ASTA Research Center, Antananarivo, Madagascar

^c Faculty of Law, Universitas Airlangga, Surabaya, Indonesia

 corresponding email : adya_pp@live.undip.ac.id

Abstract

Cybersecurity has become an important component of international aviation safety and security as the increasing digitalization of aircraft systems and air traffic management creates new risks for civil aviation. In Indonesia, the expansion of digital infrastructure in the aviation sector requires a coherent legal and institutional response to these risks. This paper aims to examine Indonesia's civil aviation cybersecurity legal framework in comparison with international standards established by the International Civil Aviation Organization (ICAO) and related legal instruments. Using a comparative doctrinal legal method, the study analyses primary legal materials, including the Aviation Law, the Electronic Information and Transactions (ITE) Law, Government Regulation No. 71 of 2019, Presidential Regulation No. 82 of 2022, and Ministerial Regulation No. 51 of 2020, supported by secondary legal materials on civil aviation cybersecurity, through normative qualitative analysis. The findings show that Indonesia has incorporated cybersecurity obligations into its aviation laws and regulations, demonstrating progress in recognizing cybersecurity as part of aviation safety and security. However, the level of compliance remains

uneven across different areas of the national legal and institutional system, particularly in institutional coordination, enforcement, and international cooperation. The study recommends strengthening the incorporation of ICAO Standards and Recommended Practices into national regulations, establishing a dedicated national aviation cybersecurity strategy, integrating cybersecurity requirements into safety and certification processes, improving cross-border cooperation and CSIRT capacity, formalizing public-private cooperation, and strengthening institutional capacity. The study concludes that Indonesia has established a substantial legal basis for aviation cybersecurity. However, greater legal coherence and institutional coordination are required to achieve more consistent compliance with international standards.

Keywords

Aviation Law, Cybersecurity, ICAO, Indonesia, International Standard Compliance.

HOW TO CITE:

Chicago Manual of Style Footnote:

¹ Adya Paramita Prabandari and Ramalina Ranaivo Mikea Manitra, “Civil Aviation Cybersecurity in Indonesia: Legal Compliance, Regulatory Gaps, and Reform in Light of ICAO Standards,” *Journal of Law and Legal Reform* 7, no 4 (2026): 2023–2066, <https://doi.org/10.15294/jllr.v7i4.40581>.

Chicago Manual of Style for Reference:

Prabandari, Adya Paramita, and Ramalina Ranaivo Mikea Manitra. “Civil Aviation Cybersecurity in Indonesia: Legal Compliance, Regulatory Gaps, and Reform in Light of ICAO Standards.” *Journal of Law and Legal Reform* 7, no 4 (2026): 2023–2066. <https://doi.org/10.15294/jllr.v7i4.40581>.

Introduction

In an era when aviation has become one of the most technologically advanced and interconnected industries, the threat of cyberattacks has become a critical importance.¹ Modern aircraft, air traffic management systems, and communication infrastructure are deeply integrated with digital networks. This reliance on technology brings significant efficiency but also exposes aviation systems to potentially serious disruption if cyber protections are inadequate. Recent studies show that aviation systems are increasingly targeted by cyberattacks such as ransomware, phishing, data breaches, unauthorized access, and distributed denial of service attacks, which may affect operational continuity, safety, and passenger privacy.² More complex attacks may involve the manipulation or spoofing of messages within communication networks. At the same time, the growing use of unmanned aerial vehicles has introduced additional risks such as channel jamming and GPS spoofing.³ These developments demonstrate that cybersecurity has become an integral element of civil aviation governance and require States to establish appropriate legal and institutional mechanisms to prevent, manage, and respond to cyber threats. The international aviation community has consequently developed a range of

¹ Tundjung Herning Sitabuana et al., “The Urgency of Artificial Intelligence Code of Ethics,” *Indonesia Law Review* 14, no. 3 (December 2024): 101–23, <https://doi.org/10.15742/ilrev.v14n3.6>.

² See, e.g., Ahmed Abdelwahab Elmarady and Kamel Rahouma, “Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment,” *IEEE Access* 9 (2021): 143997–16, <https://doi.org/10.1109/ACCESS.2021.3121230>; Haroon Malik et al., “A Homomorphic Approach for Security and Privacy Preservation of Smart Airports,” *Future Generation Computer Systems* 141 (April 2023): 500–513, <https://doi.org/10.1016/j.future.2022.12.005>.

³ See, e.g., Lázaro Florido-Benítez, “The Types of Hackers and Cyberattacks in the Aviation Industry,” *Journal of Transportation Security* 17, no. 1 (December 2024): 13, <https://doi.org/10.1007/s12198-024-00281-9>; Abiodun Esther Omolara, Moatsum Alawida, and Oludare Isaac Abiodun, “Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey,” *Neural Computing and Applications* 35, no. 31 (November 2023): 23063–101, <https://doi.org/10.1007/s00521-023-08857-7>.

instruments addressing cybersecurity within the broader framework of aviation safety and security.

The international framework has evolved from general obligations regarding the safety and security of civil aviation to more specific expectations regarding cyber resilience, safety management, information sharing, and incident response. Instruments such as the Chicago Convention and the Beijing Convention provide important legal foundations. In contrast, ICAO Annexes 17 and 19, the ICAO Cybersecurity Strategy, and related technical standards provide more specific guidance for States and aviation stakeholders. Industry standards such as RTCA DO-326A also address cybersecurity in aircraft certification, while the ICAO Cybersecurity Action Plan (2022–2025) promotes national strategies, sectoral incident response capabilities, international cooperation, and workforce development. The increasing sophistication of cyber threats, including attacks directed at critical aviation infrastructure and air traffic management systems, has strengthened the need for national frameworks to reflect these international developments.⁴ These international instruments provide an important benchmark for examining whether national legal and institutional arrangements are sufficiently prepared to address the changing cybersecurity environment.⁵

For Indonesia, significant steps have already been taken to translate the international agenda on civil aviation cybersecurity into national rules and programmes. Law No. 1 of 2009 on Aviation provides the basic framework by linking aviation safety and navigation to reliable technological systems. The Electronic Information and Transactions Law (ITE Law) complements this framework by criminalising unlawful electronic interference. Government Regulation No. 71 of 2019 further strengthens protection by designating aviation systems as part of strategic electronic infrastructure, while Presidential Regulation No. 82 of 2022 establishes aviation as a vital information infrastructure sector subject to mandatory risk management and security measures. In addition, the

⁴ Hammond Pearce, “Counterfeits and Kill Switches,” in *Futureshock* (Boca Raton: CRC Press, 2025), 154–72, <https://doi.org/10.1201/9781032702797-8>.

⁵ A detailed examination of the content and development of these international standards is provided in Section A.

National Cyber and Crypto Agency (BSSN) has introduced BSSN Regulation No. 8 of 2020, which requires strategic systems such as air traffic control to adopt internationally recognised information security standards. Ministerial Regulation No. 51 of 2020 explicitly incorporates cybersecurity obligations into aviation security programmes, showing direct alignment with ICAO's expectations. More recently, the National Aviation Safety Programme 2024–2026 confirms the government's intention to integrate cybersecurity into the broader safety framework, reflecting a forward-looking approach to managing cyber risks. These measures illustrate that Indonesia has already established a layered legal and institutional framework for aviation cybersecurity and demonstrate the government's continuing efforts to strengthen the protection of its increasingly digital aviation sector.

Nevertheless, Indonesia's civil aviation cybersecurity framework remains subject to challenges. In June 2024, the country's national data centre (*Pusat Data Nasional*) was hit by a LockBit 3.0 ransomware attack that disrupted operations at around 210 government agencies. The attack particularly affected airport immigration and passport kiosks, forcing manual processing of travellers and causing significant delays. Officials confirmed that the attackers demanded an eight-million-dollar ransom, which the government refused to pay.⁶ Around the same period, a threat actor on a dark web forum claimed to have breached the Directorate General of Civil Aviation (DGCA), allegedly obtaining about three gigabytes of sensitive data, including pilot and drone operator records, flight schedules, and staff credentials. Although the Indonesian government did not officially confirm the DGCA breach, the reported incident illustrates the potential exposure of aviation authority databases to cyber threats.⁷ Another relevant case concerns Batik Air, formerly operating as Malindo Air, where personal

⁶ Beyond Machines, "Indonesia Reports Government Data Center Hit by Ransomware," *BeyondMachines.Net*, June 24, 2024, https://beyondmachines.net/event_details/indonesia-reports-government-data-center-hit-by-ransomware-1-p-r-3-0.

⁷ Beyond Machines, "Hacker Claims Breach of Indonesian Civil Aviation Authority," *BeyondMachines.Net*, June 29, 2024, https://beyondmachines.net/event_details/hacker-claims-breach-of-indonesian-civil-aviation-authority-6-7-c-9-m.

information from a 2019 data breach reportedly resurfaced online in September 2022. The leaked database reportedly contained passengers' email addresses, dates of birth, physical addresses, passport numbers, and telephone numbers. However, the authenticity of all 45 million entries could not be verified because the database reportedly included duplicate and dummy records.⁸ These incidents provide a contemporary context for examining whether Indonesia's existing legal and institutional arrangements provide adequate protection against evolving cyber risks. The analysis of Indonesia's civil aviation cybersecurity institutional and legal framework against international standards is therefore imperative.⁹

Several recent studies have examined Indonesia's aviation cybersecurity from different perspectives. Sudarto *et al.* analyzed defense and cybersecurity in Indonesia's airspace management, identifying key threats, vulnerabilities, and mitigation efforts. Their findings indicate that despite the existence of multiple policy and technological measures, challenges remain in terms of limited skilled human resources and insufficient inter-agency coordination, which affect cyber resilience in the aviation domain.¹⁰ Lingga Dwiaji *et al.* explored the effectiveness of Indonesia's Computer Security Incident Response Team (CSIRT) in managing cyber incidents, including those affecting the aviation sector. They found that the absence of structured knowledge management and reporting mechanisms may result in repetitive cyber incidents, suggesting the need for improved organisational learning and technical

⁸ Marketing-Interactive, "Details of 45m Batik Air Customers Leaked in 2019 Reportedly Resurface Online," *Marketing-Interactive*, September 7, 2022, <https://www.marketing-interactive.com/details-of-45m-batik-air-customers-leaked-in-2019-reportedly-resurface-online>.

⁹ For the application of this assessment, readers may refer to the previous work of the authors, which employs the Global Standard Compliance framework as its main theoretical framework, a framework that is reproduced and applied in the present study to assess Indonesia's civil aviation cybersecurity. See Adya Paramita Prabandari and Ramalina Ranaivo Mikea Manitra, "Need of A Global Aviation Standard Compliance? Air Passenger Rights in Indonesia and Madagascar," *Jurnal Hukum IUS QUIA IUSTUM* 32, no. 1 (January 2025): 207–38, <https://doi.org/10.20885/iustum.vol32.iss1.art9>.

¹⁰ Sudarto, Lidia Rina Dyahtaryani, and Nanang Trianto, "Analysis of Defense and Cyber Security in Airspace Management in Indonesia," *LEX LAGUENS: Jurnal Kajian Hukum Dan Keadilan* 2, no. 2 (2024): 1–10.

infrastructure.¹¹ Hadi Prayitno *et al.* examined the transformation of Indonesia's air transportation system towards digitalisation and international compliance, stressing the importance of aligning governance, technology, and human capital with ICAO SARPs and global best practices.¹² Although these studies provide valuable insights into specific institutional and operational aspects of Indonesia's aviation cybersecurity, there remains a gap in comprehensive legal and institutional assessment against international standards.

This study offers a novel contribution by systematically assessing Indonesia's civil aviation cybersecurity against international standards. It identifies areas of strength, such as the existence of multiple laws addressing aviation cybersecurity, but also highlights weaknesses in coherence, international engagement, and enforcement¹³. The objective is twofold: first, to evaluate compliance with ICAO standards and related instruments; second, to propose policy recommendations that will enhance Indonesia's resilience against cyber threats. The findings will unfold in three steps: first, the study analyses international standards on civil aviation cybersecurity; second, it evaluates Indonesia's legal and institutional framework across its aviation laws, safety programmes, cross-sector regulations, and compliance with international standards; and lastly, it sets out policy recommendations. By combining international benchmarks with domestic analysis, this paper provides a basis for strengthening Indonesia's aviation cybersecurity framework and improving its alignment with evolving international expectations.

This study employs a comparative legal doctrinal approach to examine the legal and institutional framework governing civil aviation cybersecurity at the international and national levels. The primary legal

¹¹ Lingga Dwiaji *et al.*, "Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector," *Asian Journal of Social and Humanities* 2, no. 6 (March 2024): 1341–53, <https://doi.org/10.59888/ajosh.v2i6.261>.

¹² Hadi Prayitno, Afen Sena, and Putra Wicaksono, "Building Digital and Sustainable Transportation of Indonesia Air Transport," *Journal of Information Technology, Computer Science and Electrical Engineering* 1, no. S1 (April 2024): 26–28, <https://doi.org/10.61306/jitcse.v1iS1.14>.

¹³ Indah Sri Utari *et al.*, "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online," *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025), <https://doi.org/10.15294/ciils.v4i2.35309>.

materials include international instruments such as the Chicago Convention 1944, Annexes 17 and 19 to the Convention on International Civil Aviation, the Beijing Convention 2010, the ICAO Cybersecurity Strategy (2019), and the ICAO Cybersecurity Action Plan (2022–2025), as well as Indonesia’s domestic legal framework, comprising Law No. 1 of 2009 on Aviation, Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law) and its Law No. 19 of 2016 Amendment, Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure, BSSN Regulation No. 8 of 2020 on Cybersecurity Risk Management Guidelines, and Minister of Transportation Regulation No. 51 of 2020 on Aviation Security. The secondary legal materials consist of books, journal articles, conference proceedings, and reputable internet sources concerning civil aviation cybersecurity, international standards, Indonesian aviation governance, and relevant comparative practices. The criteria used to assess Indonesia’s compliance are established through a review of the literature on international civil aviation cybersecurity standards, as discussed in Section A of this paper, and the relevant international legal and policy instruments. The study develops the analytical criteria by triangulating the standards and requirements identified across these sources, with particular attention to aviation cybersecurity governance, risk management, safety and security oversight, airworthiness, incident response, information sharing, international cooperation, and institutional capacity. These criteria are then used as an analytical framework to compare the relevant Indonesian laws, regulations, and institutional arrangements with the identified international standards. The data analysis applies a normative qualitative approach by interpreting the relevant legal provisions and institutional arrangements against these criteria to determine the extent and consistency of Indonesia’s compliance, identify areas where the existing framework provides adequate legal and institutional support, and identify areas requiring further development. This approach allows the study to move beyond a general comparison of legal provisions by examining how the components of Indonesia’s civil aviation cybersecurity framework align with to the international standards established in the preceding analysis.

A. International Standards on Civil Aviation Cybersecurity

Aviation cybersecurity did not appear as a single rule or a single document. It grew slowly, through different kinds of legal instruments, each one built for a different purpose. Treaties imposed a duty on States to cooperate. ICAO Standards and Recommended Practices (SARPs) turned that duty into rules for national regulation. Policy instruments explained how States should apply the rules in practice, and technical standards addressed engineering and certification details. This section traces that development, from the earliest treaties to the technical standards used today, to establish the benchmark later used in this study to assess Indonesia's own framework.

1. International Treaties and Legal Obligations

The story begins with the Convention on International Civil Aviation (Chicago Convention), adopted in Chicago in 1944, which remains the foundational instrument of international civil aviation law. Article 37 asks Contracting States to cooperate so that aviation regulations, standards, and procedures stay as uniform as possible. Article 12 and related provisions place responsibility for the safety and regularity of international air navigation on States themselves. Nobody drafting the Convention in 1944 imagined cyber threats. However, these obligations still matter today, because they gave States a duty to cooperate that later standards on digital and cyber risk built upon. New generation aircraft from Boeing and Airbus depend heavily on interconnected digital systems, and where cybersecurity safeguards fall short, that dependence becomes a source of risk.¹⁴ Air traffic management shows the same pattern: as it becomes more digital and more networked, a cyber attack has more ways to cause harm.¹⁵

¹⁴ Muhammad Ali *et al.*, "Security Risk Assessments and Countermeasures for Future Aeronautical Communication Network Architecture," in *Aviation Cybersecurity: Foundations, Principles, and Applications*, ed. Houbing Song *et al.* (Bradford, United Kingdom: Institution of Engineering and Technology, 2021), 141–80.

¹⁵ LV Weiland and G Wei, "Evaluating the Impact of NextGen's Air Traffic System on Aviation Security," in *MATEC Web of Conferences*, ed. Nader Asnafi, vol. 189 (Embry Riddle Aeronautical University, United States: EDP Sciences, 2018), 10030, <https://doi.org/10.1051/mateconf/201818910030>.

A separate line of treaties addressed the criminal aspects of aviation. The Tokyo Convention 1963, the Hague Convention 1970, and the Montreal Convention 1971 required States to treat interference with aircraft as a crime. These conventions were written with hijacking and physical attacks in mind, long before anyone worried about hackers. What they left behind was a principle: States must criminalize conduct that threatens civil aviation and cooperate to stop it. When cyber threats emerged, that principle needed a new home, and it found one in the Beijing Convention and its Protocol, adopted in 2010, which extended the criminal law framework to cover new methods of attack against civil aviation, including cyber-enabled attacks.¹⁶

2. ICAO Standards and Recommended Practices

None of these treaties, however, tells a State exactly how to protect an aviation information system. That detail comes from ICAO's Annexes, and the most relevant is Annex 17, which sets international standards on aviation security. Annex 17 was originally written for physical threats, but its scope has since widened to cover information and communications technology systems used across civil aviation. States must now ensure that relevant aviation entities identify their critical ICT systems and put protective measures in place based on risk assessment, and ICAO guidance pushes States to run vulnerability assessments to check whether those measures actually work.¹⁷ The threats are real: phishing, ransomware, and denial-of-service attacks already disrupt aviation operations.¹⁸

¹⁶ See, e.g., Ruwantissa Abeyratne, "Cyber Terrorism and Aviation—National and International Responses," *Journal of Transportation Security* 4, no. 4 (December 2011): 337–49, <https://doi.org/10.1007/s12198-011-0074-3>; Michal Klenka, "Aviation Cyber Security: Legal Aspects of Cyber Threats," *Journal of Transportation Security* 14, no. 3–4 (December 2021): 177–95, <https://doi.org/10.1007/s12198-021-00232-8>.

¹⁷ Francesco Di Maio, "Centralized Security Governance for Air Navigation Services: Innovative Strategies to Confront Emerging Threats against Civil Aviation," in *2014 International Carnahan Conference on Security Technology (ICCST)*, ed. Garzia F. et al., vol. 2014-Octob (Rome, Italy: IEEE, 2014), 1–6, <https://doi.org/10.1109/CCST.2014.6986968>.

¹⁸ Masladdin M. Shueb, Chuyang Yang, and Xiaongdon Che, "An Innovative Design for Improving U.S. Airports' Cybersecurity Based on Blockchain Technology," in *2024 Systems and Information Engineering Design Symposium, SIEDS 2024*

Two more Annexes complete the picture. Annex 19, on Safety Management, requires States to run a State Safety Programme (SSP) and requires service providers to run Safety Management Systems (SMS), so that a cyber risk with safety consequences can be picked up by the same processes that already manage safety risk, a necessary link given that a cyber incident can begin as a security event and end as a direct threat to aircraft systems or air traffic management.¹⁹ Annex 10, on Aeronautical Telecommunications, protects the navigation and communication side, particularly Global Navigation Satellite Systems (GNSS), which face growing concerns over jamming and spoofing; ICAO standards and Assembly resolutions require States to protect the integrity, availability and continuity of satellite-based navigation and to prepare contingency measures, since a GNSS disruption can affect aviation safety and reach into national security more widely.²⁰ Between them, Annex 17, Annex 19 and Annex 10 cover security, safety management and technical infrastructure, the three pillars this study uses to test Indonesia's own legislation.

(United States: Institute of Electrical and Electronics Engineers Inc., 2024), 232–37, <https://doi.org/10.1109/SIEDS61124.2024.10534684>.

¹⁹ See, e.g., Marvin Blecken, Harmut Hintze, and Ralf God, “Enabling Airworthiness Security by a Holistic Security Engineering Process at Various Aircraft Design Levels,” in *ICAS Proceedings* (Hamburg, Germany: International Council of the Aeronautical Sciences, 2024), 1–12; Anna Baron Garcia, Radu F. Babiceanu, and Remzi Seker, “Means of Compliance and Relation Between Security Standards in Airworthiness Engineering,” in *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, vol. April (United States: IEEE, 2019), 1–9, <https://doi.org/10.1109/ICNSURV.2019.8735318>; Calvin Nobles, “Cyber Threats in Civil Aviation,” in *Emergency and Disaster Management*, vol. 1–3 (United States: IGI Global, 2019), 119–41, <https://doi.org/10.4018/978-1-5225-6195-8.ch007>; Calvin Nobles, “Cyber Threats in Civil Aviation,” in *Security Solutions for Hyperconnectivity and the Internet of Things* (United States Navy, Independent Researcher, United States: IGI Global, 2017), 272–301, <https://doi.org/10.4018/978-1-5225-0741-3.ch011>.

²⁰ See, e.g., Raymond Sheh, Donald Harriss, and Karen Geappen, “Autonomous Aerial Drones Connecting Public Safety: Opportunities and Challenges for the Future,” in *AUVSI XPONENTIAL* (United States: Association for Unmanned Vehicle Systems International, 2024), 1–26; Elochukwu Ukwandu et al., “Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends,” *Information* 13, no. 3 (March 2022): 1–22, <https://doi.org/10.3390/info13030146>.

3. ICAO Cybersecurity Strategy, Action Plan and Other Policy Instruments

While the Annexes provide binding rules, ICAO's policy instruments give provide direction. The Aviation Cybersecurity Strategy, adopted in 2019, was the first document to bring the main elements of aviation cybersecurity under one roof: international cooperation, governance, effective legislation, information sharing, incident management, and capacity building²¹. It carries no binding force, but it tells States what cybersecurity should look like in practice. It makes a simple point that runs throughout the rest of this framework: aviation authorities cannot manage cybersecurity alone. They need cybersecurity institutions, industry and other stakeholders working with them, because secure communication between aircraft, ground infrastructure and international partners is what keeps modern aviation interoperable.²² The Cybersecurity Action Plan for 2022 to 2025 then turned this strategy into something more concrete: sector-specific Computer Security Incident Response Teams (CSIRTs), cyber resilience built into certification and oversight, stronger international cooperation and a trained workforce, all while regulators try to keep pace with new technologies such as artificial intelligence.²³ A third instrument, the

²¹ Baiq Farhatul Wahidah, Rizkiati Khasanah, and Fadly Husain, "Anatomical Traits and Economic Potential of *Amorphophallus Variabilis* and Conservation Implications in Selo Arjuno Forest, Central Java, Indonesia," *Biodiversitas* 27, no. 2 (2026), <https://doi.org/10.13057/biodiv/d270213>.

²² See, e.g., Madhu Niraula, "Cybersecurity and Interoperability of Aviation Safety Service Ecosystem," in *Integrated Communication, Navigation and Surveillance Conference (ICNS)*, vol. April (United States: IEEE, 2022), 1–12, <https://doi.org/10.1109/ICNS54818.2022.9771482>; Regner Sabillon and Juan Ramon Bermejo Higuera, "The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities," in *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, ed. Degen H., Ntoa S., and Moallem A., vol. 14059 LNCS (Logroño, Spain: Springer Science and Business Media Deutschland GmbH, 2023), 461–79, https://doi.org/10.1007/978-3-031-48057-7_29; Klenka, "Aviation Cyber Security: Legal Aspects of Cyber Threats."

²³ Tuncel Oz, "Cybersecurity as a Strategic Lever for Innovation in Smart Aviation Ecosystems: A Review of Emerging Trends," in *Utilizing Cybersecurity to Foster Business Innovation and Resiliency*, ed. Filiz Mızrak (Istanbul Ticaret University,

Global Air Navigation Plan (GANP), takes a narrower angle: it builds cybersecurity into the Aviation System Block Upgrades and asks States to think about cyber protection whenever they add digital, networked technology to air navigation, because reliable communication between aircraft, ground systems and international partners underpins modern air traffic management.²⁴

Beneath these policy instruments sit ICAO's operational manuals. The Aviation Security Manual (Doc 8973) and the Air Traffic Management Security Manual (Doc 9985) give States practical guidance on cyber threats, information sharing, incident reporting, vulnerability assessment and incident response, and practices such as penetration testing put that guidance into action.²⁵ Even the best-written standard is worth little without the capacity to apply it, which is where ICAO's No Country Left Behind (NCLB) initiative comes in. It covers aviation standards broadly, not cybersecurity alone, but it offers technical assistance, training, and capacity building to States implementing ICAO SARPs, and that support matters because compliance depends as much on trained personnel and technical expertise as it does on the law itself, particularly as aviation adopts artificial intelligence and digital twins.²⁶

Turkey: IGI Global, 2025), 103–22, <https://doi.org/10.4018/979-8-3693-6417-8.ch005>.

²⁴ Weiland and Wei, “Evaluating the Impact of NextGen's Air Traffic System on Aviation Security.”

²⁵ See, e.g., Branislav Kanderka *et al.*, “Supply Chain Risks Assessment of Selected EUROCONTROL's Surveillance Products,” in *2022 New Trends in Aviation Development (NTAD)*, ed. Andoga R. and Fozo L. (Žilina, Slovakia: IEEE, 2022), 86–89, <https://doi.org/10.1109/NTAD57912.2022.10013524>; Filiz Mizrak and Gonca Reyhan Akkartal, “Prioritizing Cybersecurity Initiatives in Aviation: A Dematel-QSFS Methodology,” *Heliyon* 10, no. 16 (August 2024): e35487, <https://doi.org/10.1016/j.heliyon.2024.e35487>.

²⁶ See, e.g., Mahmaud Eleimat, Omar Alharasees, and Arnold Oszi, “Advancements in Airport Security Technologies: A Patent Analysis,” in *Proceedings of 2024 1st Edition of the Mediterranean Smart Cities Conference, MSCC 2024*, ed. Dahmane A.B. *et al.* (Budapest, Hungary: Institute of Electrical and Electronics Engineers Inc., 2024), <https://doi.org/10.1109/MSCC62288.2024.10696990>; Cengiz Kerem Kutahya, “Securing the Digital Twin: Cybersecurity Strategies for Virtual Replicas in Aviation Management,” in *Utilizing Cybersecurity to Foster Business Innovation and Resiliency*, ed. Filiz Mizrak (IGI Global, 2025), 241–60, <https://doi.org/10.4018/979-8-3693-6417-8.ch011>; Sabillon and Bermejo

4. Technical and Cross-Sectoral Cybersecurity Standards

Some of the most detailed cybersecurity work happens entirely outside ICAO. RTCA DO-326A, read with DO-356A and DO-355, gives aircraft manufacturers a certification framework covering threat assessment, security requirements, design, verification, and continuing airworthiness. These are not treaties or SARPs, but regulators treat them as the accepted way to demonstrate that an aircraft meets airworthiness security expectations, and researchers argue that this work should start early in the design process and keep updating as threats change.²⁷ As aircraft depend more on interconnected communication systems, secure authentication becomes part of that same design task.²⁸

Aviation cybersecurity does not stop at the edge of aviation law. The Council of Europe Convention on Cybercrime, known as the Budapest Convention, criminalizes offenses such as illegal access to computer systems and interference with data, and sets up mechanisms for cross-border criminal cooperation; it says nothing about aircraft specifically, but an attack on aviation infrastructure often involves perpetrators, systems, and evidence spread across several States, so a general cybercrime treaty becomes relevant in practice. Indonesia has not joined the Budapest Convention, while the United States has.²⁹ The

Higuera, “The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities.”

²⁷ See, e.g., Sanghoon Jeon, “Improvement Measures for Aviation Security Policies and Security Management System Against Potential Cyber Threats In-Flight,” *The Journal of Korean Institute of Communications and Information Sciences* 48, no. 11 (November 2023): 1525–33, <https://doi.org/10.7840/kics.2023.48.11.1525>; Christoph Torens, “Safety versus Security in Aviation, Comparing Do-178c with Security Standards,” in *ALAA Scitech 2020 Forum*, vol. 1 PartF (Braunschweig, Germany: American Institute of Aeronautics and Astronautics Inc, AIAA, 2020), 1–12, <https://doi.org/10.2514/6.2020-0242>.

²⁸ Nils Maurer *et al.*, “PMAKE: Physical Unclonable Function-Based Mutual Authentication Key Exchange Scheme for Digital Aeronautical Communications,” in *Proceedings of the IM 2021 - 2021 IFIP/IEEE International Symposium on Integrated Network Management*, ed. Ahmed T. *et al.* (Wessling, Germany: Institute of Electrical and Electronics Engineers Inc., 2021), 206–14.

²⁹ See, e.g., Elmarady and Rahouma, “Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment”; Shueb, Yang, and Che, “An Innovative Design for Improving U.S. Airports’ Cybersecurity Based on Blockchain Technology”; Sabillon and Bermejo Higuera,

International Telecommunication Union (ITU) works from a different angle, encouraging States to build national cybersecurity strategies and Computer Incident Response Teams; aviation authorities sit inside these wider national structures, and cooperation with them supports incident response and information sharing at a national level.³⁰ Regional bodies add a further, more local layer: the European Civil Aviation Conference adopted its Strategic Roadmap for Aviation Cybersecurity in 2019, and ICAO's regional security coordination mechanisms in the Asia Pacific support information exchange and training, giving Indonesia a route to build capacity within its own region.³¹

What emerges from this section analysis is a framework built in stages, over many years, not designed at once. The Chicago Convention and its related treaties imposed a duty on States to cooperate. The Annexes turned that duty into standards for security, safety, and technical infrastructure. The Strategy, the Action Plan, and the GANP gave States direction on how to apply those standards, and technical standards such as RTCA DO-326A carried cybersecurity into aircraft design itself. Cybercrime and telecommunications instruments then connected aviation to the wider legal and institutional world on which it depends on. It is this layered structure that the following section uses to examine Indonesia's own legal and institutional framework.

Figure 1 presents the analytical framework used in this study to identify the main international standards for civil aviation cybersecurity. The framework brings together ten interrelated areas, covering treaty obligations and ICAO SARPs, national cybersecurity strategies, safety management, airworthiness, criminal law and cross border cooperation,

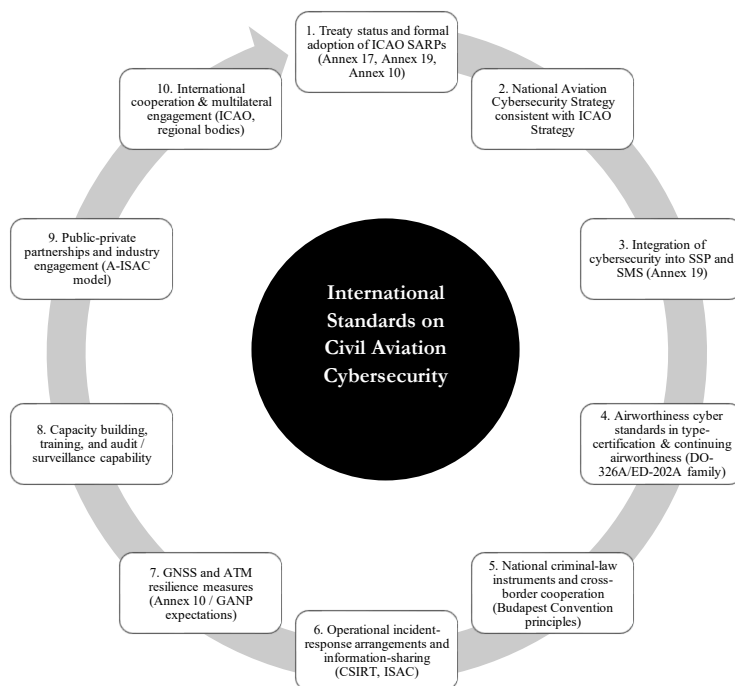
"The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities."

³⁰ See, e.g., Garcia, Babiceanu, and Seker, "Means of Compliance and Relation Between Security Standards in Airworthiness Engineering"; Kutahya, "Securing the Digital Twin: Cybersecurity Strategies for Virtual Replicas in Aviation Management."

³¹ See, e.g., Imdad Ali Shah, N. Z. Jhanjhi, and Sarfraz Brohi, "Cybersecurity Issues and Challenges in Civil Aviation Security," in *Cybersecurity in the Transportation Industry*, ed. Imdad Ali Shah and Noor Zaman Jhanjhi (Kuala Lumpur, Malaysia: Wiley, 2024), 1–23, <https://doi.org/10.1002/9781394204472.ch1>; Nobles, "Cyber Threats in Civil Aviation," 2017; Ukwandu et al., "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends."

incident response and information sharing, GNSS and air traffic management resilience, capacity building and oversight, public private cooperation, and international engagement.³² These elements provide the benchmarks used in this study to assess the extent to which Indonesia's legal and institutional framework corresponds with international expectations on civil aviation cybersecurity.

Figure 1. International Standards on Civil Aviation Cybersecurity



Source: Authors' analysis

³² For understanding on international cooperation, *see compare* Hendronoto Soesabdo et al., "Global Competition Law Beyond Treaties: The Rise and Limits of Networks," *Juridical Tribune-Review of Comparative & International Law* 16, no. 2 (2026): 204–23. *See also* Maminirina Fenitra Rakotoarisoa, Heni Kurniasih, and Mikea Manitra Ramalina Ranaivo, "Advancing Regional Cooperation to Combat Marine Debris and Enhance Livelihoods in Indonesia: Translating Global Agendas into Local Action," *Marine Pollution Bulletin* 224 (March 2026): 119097, <https://doi.org/10.1016/j.marpolbul.2025.119097>.

B. Indonesia's Civil Aviation Cybersecurity Legal and Institutional Framework

Indonesia has developed a multi-layered legal and institutional framework for civil aviation cybersecurity. The foundation is laid down in sectoral aviation law, complemented by general electronic information law, cyber-infrastructure protection regulations, and specific ministerial instruments. These rules impose obligations on both the state and aviation operators and allocate supervisory and enforcement powers to various institutions. However, as Agus Bhakti *et al.* point out, Indonesia's cyber defence policies remain fragmented due to overlapping authorities, which weakens coherence in the aviation context.³³ In response, the DGCA has begun revising the National Civil Aviation Security Programme to strengthen coordination, including a categorisation of operators based on their ability to handle cyber incidents and requirements for each to establish a CSIRT registered with BSSN.³⁴

1. Aviation Law Provisions and Operational Reliability

Law No. 1 of 2009 on Aviation is the starting point. It lays the legal foundation for aviation safety, security, navigation, and operational reliability in Indonesia.³⁵ Article 269 defines air navigation services around compliance with standards, efficiency, and an integrated national and international network, and Article 270 places air traffic services and aeronautical telecommunication services among the main categories of air navigation. None of these uses the term "cybersecurity". Nevertheless, the emphasis on reliable and integrated navigation and communication systems gives Indonesia a legal basis for protecting the digital systems on which these services now run. ICAO Annex 19 asks States to build

³³ Agus Bhakti *et al.*, "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia," *Journal of Human Security* 20, no. 1 (2024): 109–17, <https://doi.org/10.12924/johs2024.20116>.

³⁴ Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration," ICAO, 2025.

³⁵ Puan Maharani Kusumadewi *et al.*, "Analisis Standar Penerbangan Di Indonesia Berdasarkan Hukum Udara Internasional," *Masalah-Masalah Hukum* 52, no. 3 (October 2024): 262–71, <https://doi.org/10.14710/mmh.52.3.2023.262-271>.

systematic safety risk management through State Safety Programmes (SSPs) and Safety Management Systems (SMSs); the Aviation Law supplies the underlying statutory requirement for reliable operations, but stops short of a specific cyber risk management mechanism within the statute itself. Private operators sit close to this gap, since much of aviation service delivery runs through private technological and operational providers, which is why Pradipta N. Saputra *et al.* stress public-private partnerships as part of Indonesia's cybersecurity governance.³⁶ The DGCA has already moved in that direction, running workshops and table-top exercises with the Australian Government that bring aviation stakeholders into the room.³⁷

Article 272(3) of the same Law requires service providers to establish standard operating procedures, maintain reliable systems, employ licensed personnel, and run quality assurance mechanisms. Article 297 requires that navigation facilities be installed with technological development and system reliability in mind. Neither article mentions cybersecurity, and a disruption or unauthorized interference with aviation systems can still directly affect operational safety through them. What is missing is the specific machinery ICAO Annex 17 requires: a cyber risk assessment, the identification of critical ICT systems, and the identification of protective measures. The National Aviation Safety Program (NASP) 2024–2026 closes some of that gap directly, requiring airlines, airports, and air navigation service providers to identify critical ICT systems, risk assessments, and put protective measures in place,³⁶ which pulls Indonesia's operational framework closer to the risk-based approach in Annex 17 and Annex 19. Editha Pradipta *et al.* make a related point: national cybersecurity policy only works once it is translated into effective sectoral implementation.³⁷ Radio frequency provisions in Law No. 1 of 2009 protect aviation communications on a separate track. Article 302 restricts aeronautical frequencies to purposes connected with flight safety, and Article 306 prohibits activities that may interfere with aviation safety. Set against

³⁶ Pradipta Nindyan Saputra *et al.*, "Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)," *Central European Journal of International and Security Studies* 13, no. 4 (2019): 104–20.

³⁷ Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration."

ICAO Annex 10, which governs aeronautical telecommunications and the reliability and continuity of communication and navigation systems, these articles give Indonesia a legal basis for preventing harmful electronic interference, including interference that reaches aviation communications. The NASP 2024–2026 pushes this further, tying aviation ICT security to critical infrastructure resilience and to protecting the confidentiality, integrity and availability of aviation information systems.³⁸

2. Safety and Security Programmes, Airworthiness, and Institutional Roles

Safety management is embedded in Law No. 1 of 2009 itself. Article 308 puts the Minister of Transport in charge of establishing a State Safety Programme (SSP), Article 309(1) requires that programme to cover reporting, data analysis, safety information exchange and enforcement, and Articles 317 to 321 require operators to run Safety Management Systems (SMS), including incident reporting and auditing. Because a cyber incident can affect the safety of aircraft, navigation systems, and aviation operations just as easily as a mechanical fault can, these provisions already provide Indonesia with a legal basis for integrating cyber incidents into aviation safety management. ICAO Annex 19 asks States and service providers to identify and manage safety risks through structured processes, and here the Indonesian framework falls short in one respect: cybersecurity is not named as a defined category of safety risk. Rakha Wilis and Jackson Sidabutar find a related gap at the institutional level, where incident response through Indonesia's national CSIRT remains largely reactive and existing CSIRT arrangements have not been fully optimized for aviation-specific threats.³⁹ The DGCA has begun testing crisis communication, decision-making, and coordination

³⁸ Ministry of Transportation - Republic of Indonesia, "National Aviation Safety Plan 2024-2026," ICAO, 2024.

³⁹ Rakha Wilis and Jackson Sidabutar, "How Can Gov-CSIRT Indonesia Maintain National Cybersecurity in the Future?," in *2024 16th International Conference on Information Technology and Electrical Engineering (ICITEE)* (Bogor, Indonesia: IEEE, 2024), 440–45, <https://doi.org/10.1109/ICITEE62483.2024.10808204>.

between relevant actors through recent aviation cybersecurity table-top exercises.⁴⁰

The security framework speaks to cybersecurity more directly. Articles 323 to 327 of Law No. 1 of 2009 place the Minister in charge of establishing a National Aviation Security Programme that covers the protection of airports, aircraft, and navigation facilities, as well as responses to unlawful interference, and require that training, auditing, and international cooperation accompany it. This aligns with ICAO Annex 17, which requires States to implement measures against unlawful interference and maintain appropriate security systems. Minister of Transportation Regulation No. 51 of 2020 on National Aviation Security goes a step further: Article 24 expressly requires providers of aviation electronic systems to implement cybersecurity measures in line with the national aviation security programme, arguably the clearest point of correspondence between Indonesian law and international aviation cybersecurity expectations. The scope stays narrower than the international approach, though, which treats cybersecurity as continuous risk assessment, incident response, information sharing and institutional cooperation running across the whole sector, and cybersecurity responsibilities here are split between aviation authorities, operators and national cyber institutions. A. Fathan Taufik points to limitations in Indonesia's cyber diplomacy and international cooperation,⁴¹ though Indonesia's participation in ICAO and ASEAN aviation cybersecurity initiatives, and its willingness to run joint table-top exercises, suggest that engagement is growing.⁴²

Airworthiness tells a different story. Law No. 1 of 2009 sets out a full regime for aircraft registration and certification: Article 22 requires any aircraft operating in Indonesia to hold registration and a certificate of airworthiness, Article 23 lets that certificate issue only after inspection

⁴⁰ Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration."

⁴¹ A Fathan Taufik, "Indonesia's Cyber Diplomacy Strategy as a Deterrence Means to Face the Threat in the Indo-Pacific Region," *Journal of Physics: Conference Series* 1721, no. 1 (January 2021): 012048, <https://doi.org/10.1088/1742-6596/1721/1/012048>.

⁴² Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration."

by authorised officials or designated entities, Article 24 makes its continued validity conditional on ongoing compliance, Article 25 requires continuous maintenance by certified maintenance organisations, and Article 26 lets the Minister strike an aircraft from the national register once the conditions for continued airworthiness stop being met. Government Regulation No. 32 of 2021 on Aviation Operations and Minister of Transportation Regulation No. 62 of 2021 on Aircraft Certification and Airworthiness carry this into practice: Articles 54 and 55 of the Government Regulation, read with Articles 3 and 5 of the Ministerial Regulation, cover certification, maintenance, damage, repairs and modifications, and Articles 56 to 58 of the Government Regulation, read with Articles 6 and 7 of the Ministerial Regulation, deal with the validity and recognition of airworthiness certificates, foreign aircraft included. What results is a structured system for the technical integrity of aircraft, consistent with the airworthiness obligations in the Chicago Convention and ICAO standards.⁴³ Cybersecurity is where the structure runs out: the Indonesian airworthiness provisions stay focused on the physical and technical condition of aircraft, with no express requirement for cyber risk assessment, protection of aircraft digital systems, or cybersecurity in certification and continuing airworthiness. Industry standards such as RTCA DO-326A/ED-202A already treat cybersecurity as part of aircraft development and continuing airworthiness, a step Indonesian airworthiness law has not yet taken.

These three areas show that Indonesia is not short of a legal foundation for aviation cybersecurity. Safety management, aviation security, incident reporting, operational reliability, and airworthiness certification all offer an entry point. What varies is how far cybersecurity is written into each one, expressly and systematically: the aviation security framework names it most directly, whereas the SSP and SMS frameworks can manage cyber risk without ever defining it as a distinct category of safety risk. Airworthiness regulation remains focused on technical certification while excluding cybersecurity from continuing

⁴³ Bryan Dennis Longdong, “Pengaturan Hukum Mengenai Pendaftaran Pesawat Udara Menurut Undang-Undang No 1 Tahun 2009 Tentang Penerbangan,” *Lex Privatum* 9, no. 3 (2021): 151–61.

airworthiness. Compliance, on this evidence, cannot be read off the existence of legislation alone; it depends on whether each provision's substance aligns with the specific international expectations for prevention, risk management, incident response, technical resilience, and institutional coordination.

3. Cross-Sectoral Cyber Laws and Institutional Coordination

a. Substantive Cybersecurity Obligations

Aviation cybersecurity in Indonesia does not rest solely on aviation law; general legislation on electronic systems and critical information infrastructure supports it. Law No. 19 of 2016, which amended the Electronic Information and Transactions Law (ITE Law), criminalises unauthorised interception of electronic transmissions under Article 31, requires the Government under Article 40 to protect the public interest from the misuse of information technology and gives a basis for identifying electronic systems holding strategic data that need protection, and grants investigative powers under Article 43 to the police and authorised civil servants responsible for electronic systems. Between them, these articles cover unlawful access, interception, and interference involving aviation-related electronic systems, at least in general terms. How well they work depends on whether enough people with real cybersecurity expertise are around to apply them. Saputra *et al.* flag the shortage of trained cyber personnel as a concern across Indonesia's wider cybersecurity framework.⁴⁴ The National Aviation Safety Plan (NASP) 2024–2026 answers this directly in the aviation sector, promoting specialized training and cyber incident response capacity among aviation personnel.⁴⁵

Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions adds a further layer, this time specifically aimed at strategic electronic

⁴⁴ Saputra *et al.*, "Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)."

⁴⁵ Ministry of Transportation - Republic of Indonesia, "National Aviation Safety Plan 2024-2026"; Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration."

systems. Article 28 defines a strategic electronic system by the consequences of its disruption for national interests; Article 29 requires its operator to maintain security, report serious incidents, conduct audits, and keep the service running; and Articles 20 to 23 cover confidentiality, risk management, and recovery from disruption. Aviation systems fit squarely within this definition, since their disruption directly affects the continuity of air transport services. Praditya *et al.* note that Indonesia's cybersecurity resilience measures still need stronger implementation and regular auditing, a gap that matters here as much as anywhere.⁴⁶

Presidential Regulation No. 82 of 2022 on the Protection of Vital Information Infrastructure expressly names transport as one of the sectors covered by the national vital information infrastructure regime. Article 4 makes transport a strategic sector, Article 9 requires operators to apply information security standards, Article 10 requires risk management, Articles 11 to 17 set up incident response at national, sectoral and organizational levels with a twenty-four-hour reporting obligation, and Articles 23 to 25 give BSSN a coordinating role across all of it. As a result, aviation-related information systems sit within this broader national cybersecurity architecture. BSSN Regulation No. 8 of 2020 fills in the technical detail, classifying electronic systems by risk under Article 6, requiring strategic electronic systems to adopt ISO/IEC 27001 standards under Article 9, providing for certification and periodic audits under Articles 26 to 34, and giving BSSN its supervisory role under Articles 35 and 36. Between the two regulations, Indonesia's approach moves beyond the simple criminalization of cyber offenses and into preventive territory: risk management, certification, auditing, and incident response.

One gap sits outside the domestic framework altogether. Indonesia has not acceded to the Budapest Convention on

⁴⁶ Editha Praditya et al., "National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence," *Journal of Human Security* 19, no. 2 (2023): 91–106, <https://doi.org/10.12924/johs2023.19020012>.

Cybercrime or the Beijing Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation, which keeps its domestic framework at arm's length from the established international mechanisms for cooperating on cybercrime investigation and aviation-related offences.⁴⁷ That absence bites hardest where cyber incidents cross borders, foreign actors, overseas service providers, or data sitting outside Indonesia among the likely complications.⁴⁸ Indonesia's cross-sectoral framework gives it a substantial domestic basis for protecting aviation information systems; how far it connects to the international legal architecture remains a separate question, one this study returns to in assessing compliance.

b. Institutional Coordination and Implementation

Making these obligations work in practice comes down to several institutions pulling together. The Ministry of Transportation, through the DGCA, handles aviation-specific regulation and oversight; BSSN sets national cybersecurity standards and coordinates supervision and incident response; the Ministry of Communication and Information Technology carries broader responsibility for electronic systems; the national police cyber unit handles criminal investigation. Airlines, airport operators, and air navigation service providers are left to implement the applicable security measures inside their own systems.

Splitting responsibility among four institutions places greater weight on coordination. Wilis and Sidabutar find the

⁴⁷ Adya Paramita Prabandari and Efrema Ardratya Prakasita Puteri, "Standardization of Private Aircraft: Implications of Climate Change," in *IOP Conference Series: Earth and Environmental Science*, vol. 1270 (Indonesia: Institute of Physics, 2023), 012028, <https://doi.org/10.1088/1755-1315/1270/1/012028>.

⁴⁸ This could even be problematic in times of war. *See, e.g.*, Ramalina Ranaivo Mikea Manitra et al., "Vanishing Universal Norms? Rethinking Erga Omnes in International Humanitarian Law Principles," *Brawijaya Law Journal* 12, no. 2 (October 2025): 257–81, <https://doi.org/10.21776/ub.blj.2025.012.02.04>; Ramalina Ranaivo Mikea Manitra and Adya Paramita Prabandari, "AI in Hybrid Conflicts: Towards a Legal Framework for Cognitive Warfare," *Cogent Social Sciences* 12, no. 1 (December 2026): 1–24, <https://doi.org/10.1080/23311886.2026.2681304>.

national CSIRT framework still needs stronger mechanisms for incident reporting and coordinated response.⁴⁹ Aviation has taken some concrete steps of its own: the DGCA Directorate of Aviation Security now sits as the CSIRT Liaison for air transport. It participates in BSSN's Information Sharing and Analysis Center for Aviation Security (ISACS) forum, effective from 2025.⁵⁰ Joint workshops between the DGCA, BSSN, and aviation stakeholders have produced regulatory and technical guidance built through consultation with operators.⁴⁹

Private actors bear much of this weight in practice. Airlines, airports, air navigation service providers, technology companies and other private operators run systems that make up much of the wider aviation infrastructure, which is why Saputra *et al.* argue that stronger public-private partnerships are necessary for Indonesia's cybersecurity governance.⁵⁰ The NASP 2024–2026 pushes in the same direction, promoting cooperation between government institutions, industry and technology providers as part of aviation safety and cybersecurity capacity building.⁵¹ Whether these institutional arrangements actually work will show up in how closely responsibilities, information-sharing mechanisms, incident reporting and oversight match the international standards this study examines.

4. Assessment of Compliance with International Standards on Civil Aviation Cybersecurity

The previous section (section A) has outlined the key international standards governing aviation cybersecurity, including binding treaty obligations and non-binding ICAO strategies and guidance. Since these standards serve as the global benchmark for state practice, it is important to assess how far Indonesia's legal and institutional framework aligns with them. Such an assessment allows us to identify both the strengths

⁴⁹ Republic of Indonesia, "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration."

⁵⁰ Saputra *et al.*, "Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)."

⁵¹ Ministry of Transportation - Republic of Indonesia, "National Aviation Safety Plan 2024-2026."

and the weaknesses of Indonesia’s current system in relation to its international obligations. The table below provides a structured summary of Indonesia’s compliance with those standards, serving as the basis for a more detailed analysis of its achievements and shortcomings.

Table 1. Indonesia’s Compliance with International Standards on Civil Aviation Cybersecurity

Variable (ICAO expectation)	Compliance	Evidence (from Indonesian framework)	Strengths	Weaknesses
1. Treaty status and formal adoption of ICAO SARPs (Annex 17, Annex 19, Annex 10)	✓ High	Indonesia is ICAO Contracting State; NASP 2024–2026 explicitly aligns with Annex 17 and Annex 19	Clear formal alignment, NASP explicitly references ICAO SARPs.	Implementation gaps at operational level remain.
2. National Aviation Cybersecurity Strategy consistent with ICAO Strategy	≈ Medium	Cyber requirements now embedded in NASP 2024–2026; DGCA revising NCASP; BSSN coordination under Presidential Reg 82/2022.	Formal strategy elements exist, cross-agency instruments created.	Fragmentation across agencies, strategy still recent and maturing.
3. Integration of cybersecurity into SSP and SMS (Annex 19)	≈ Medium	Law No.1/2009 requires SSP/SMS; NASP mandates incident reporting and risk assessments	Legal basis for SSP/SMS integration into safety oversight.	SMS/SSP practice still reactive; CSIRT integration not fully mature.
4. Airworthiness cyber standards in type-certification & continuing airworthiness (DO-326A/ED-202A family)	✗ Low	Airworthiness law and regs (Gov Reg 32/2021; Ministerial Reg 62/2021) set certification regime, but no explicit cybersecurity standards referenced.	Strong procedural airworthiness regime generally compliant with Chicago Convention.	No explicit adoption or mandatory use of DO-326A/ED-202A in certification process.

5. National criminal-law instruments and cross-border cooperation (Budapest Convention principles and 2010 Beijing Convention)	≈ Medium	ITE Law (No.19/2016) criminalises unauthorised access; Indonesia has investigatory powers; Indonesia not a Party to Budapest Convention nor 2010 Beijing Convention.	Domestic criminal provisions exist to prosecute cyber offences.	Limited structured cross-border legal tools, capacity gaps for transnational investigations.
6. Operational incident-response arrangements and information-sharing (CSIRT, ISAC)	≈ Medium	Presidential Reg 82/2022 requires sectoral CSIRTs; DGCA requiring operator CSIRTs registered with BSSN; BSSN ISACS participation started in 2025 (DGCA paper, 2025).	Formal CSIRT architecture, recent registration and ISAC linkage, TTX exercises performed.	CSIRT maturity, timeliness of reporting, and two-way operational sharing remain limited.
7. GNSS and ATM resilience measures (Annex 10 / GANP expectations)	≈ Medium	Aviation designated strategic under Gov Reg 71/2019 and Pres. Reg 82/2022; NASP references critical ICT and contingency planning.	Policy recognition of GNSS/ATM as critical, risk management obligations exist.	Technical resilience gaps noted for satellite and national data centre protection.
8. Capacity building, training, and audit / surveillance capability	≈ Medium	NASP mandates training, DGCA-BSSN maturity assessments, NCLB/ICAO assistance used.	Commitment to training and international cooperation, recent TTX and workshops.	Shortage of specialised cyber personnel, audits and enforcement still developing.
9. Public-private partnerships and industry engagement (A-ISAC model)	≈ Medium	NASP calls for PPP, DGCA engaged private operators, workshops with industry and Australia TTX.	Growing PPP rhetoric and practical engagement in exercises.	Formalised, contractual PPP frameworks and incentives not yet widespread.

10. International cooperation & multilateral engagement (ICAO, regional bodies)	✓ High	Active engagement, participation in APAC forums, NCLB and ICAO technical cooperation access, bilateral exercises with Australia.	ICAO	Strong international engagement, access to ICAO support and capacity building.	Technology transfer and deep operational partnerships still limited in some areas.
---	--------	--	------	--	--

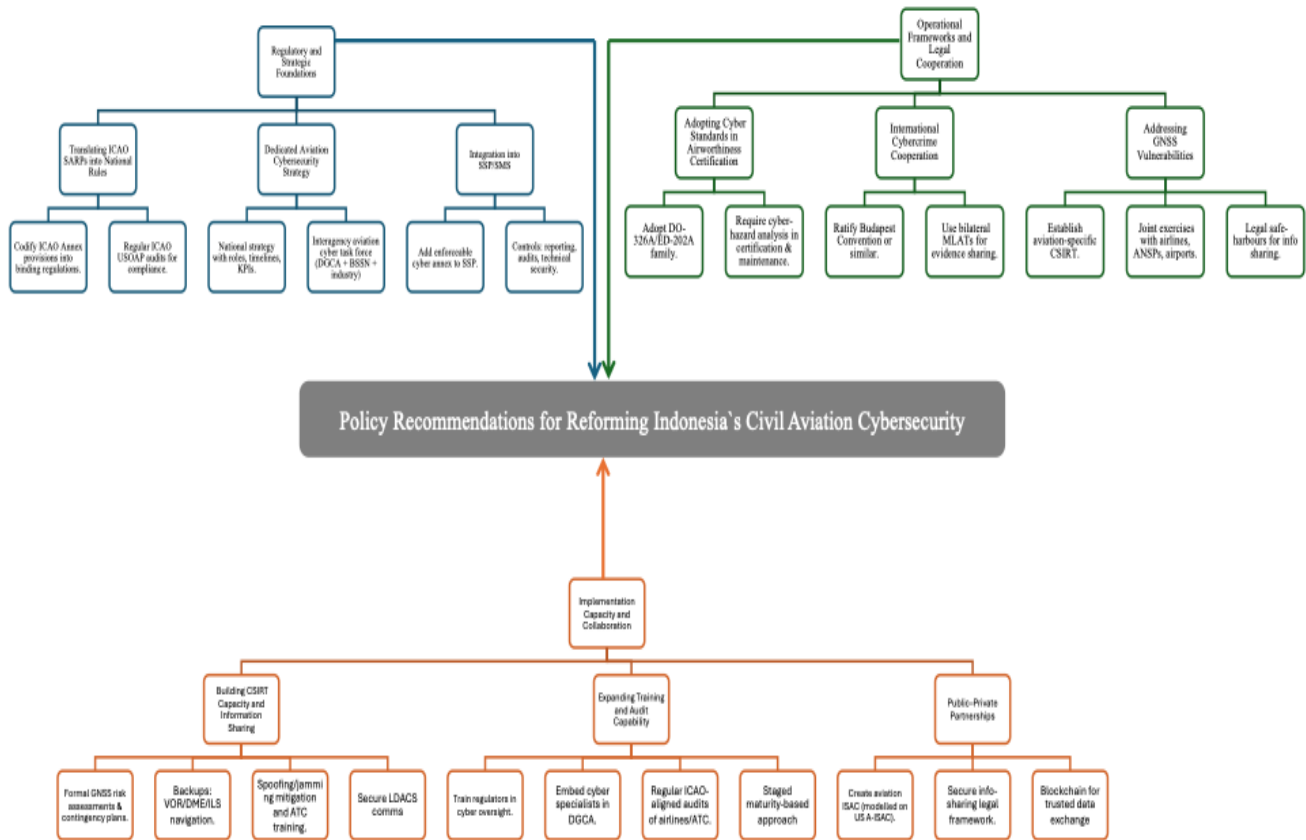
Source: Authors’ analysis

Table 1 shows that Indonesia has achieved solid formal alignment with ICAO standards and has developed a comprehensive legal scaffolding. However, important operational and technical gaps remain, notably in airworthiness cyber-certification, CSIRT maturity, specialist workforce capacity, and structured cross-border cooperation. In consequence, priority reforms should focus on translating NASP commitments into mandatory certification criteria, accelerating CSIRT capability and exercises, scaling regulator and industry training, and pursuing stronger international legal instruments for cross-border investigations.

C. Policy Recommendations for Reforming Indonesia’s Civil Aviation Cybersecurity

Indonesia has built a substantial legal and institutional framework for civil aviation cybersecurity, but gaps remain in coherence, implementation, enforcement, and international cooperation. Closing them means turning existing commitments into clearer operational requirements and better coordination between aviation and cybersecurity institutions. Drawing on the compliance assessment and comparative practices from other jurisdictions, six areas of reform are proposed below: translating international standards into national rules, establishing a dedicated aviation cybersecurity strategy, integrating cybersecurity into safety and airworthiness systems, strengthening international cybercrime cooperation, improving incident response and technical resilience, and developing institutional capacity and public-private cooperation (see its operationalization in Figure 2).

Figure 2. Policy Recommendations for Reforming Indonesia’s Civil Aviation Cybersecurity



Source: Authors’ analysis

1. Translating ICAO Standards into Binding National Rules

Indonesia should continue translating relevant ICAO Standards and Recommended Practices (SARPs) into binding national rules, and it needs a regular mechanism to review their implementation. The European Union offers one model: EASA and the European Commission incorporate international aviation standards into regional legislation and then follow through with regulatory oversight. The United States runs a comparable process, reviewing ICAO amendments to work out what they mean for domestic regulation. Indonesia could build something similar under the DGCA, mapping each relevant ICAO cybersecurity requirement against an existing Indonesian regulation, the institution responsible for it, its implementation status, and how it is enforced. This would reduce inconsistencies across regulations and make it easier to spot provisions that were formally adopted but never properly implemented. A risk-based, system-wide approach matters here because aviation cybersecurity depends on how aircraft, airports, air navigation services, information systems, and other connected infrastructure interact with one another.⁵²

2. Establishing a Dedicated Aviation Cybersecurity Strategy

Indonesia needs a dedicated national civil aviation cybersecurity strategy, one that allocates responsibilities clearly, sets implementation priorities, and gives measurable targets. The UAE's National Civil Aviation Cybersecurity Strategy is a useful comparison: it ties aviation cybersecurity to the country's broader national cybersecurity framework. It sets out measures covering regulation, institutional responsibilities, and workforce development. In Indonesia's case, such a strategy could establish a formal coordination mechanism bringing together the DGCA, BSSN, airport operators, airlines, air navigation service providers, and relevant technology providers, with regular risk assessments and defined requirements for incident reporting, audits, training, and infrastructure protection. That would give a single policy direction to rules currently scattered across aviation, cybersecurity, and

⁵² Georgia Lykou, George Iakovakis, and Dimitris Gritzalis, "Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management," in *Advanced Sciences and Technologies for Security Applications* (Athens, Greece: Springer, 2019), 245–60, https://doi.org/10.1007/978-3-030-00024-0_13.

electronic information regulations. Systematic risk assessment matters because it lets cybersecurity risks be judged by their potential impact on aviation safety and operational continuity.⁵³

3. Integrating Cybersecurity into Safety Management and Airworthiness

Cybersecurity should be explicitly embedded within Indonesia's State Safety Program (SSP), Safety Management Systems (SMS), and airworthiness certification framework. A dedicated cybersecurity component within the SSP could set minimum requirements for cyber-risk identification, incident reporting, vulnerability assessment, and oversight, and cybersecurity controls should become a routine part of safety inspections and audits. Europe and the United States already treat cybersecurity as an operational risk requiring specialized institutional oversight; Indonesia should assess cyber risks alongside other safety risks in the same way, instead of leaving them mainly to separate cybersecurity regulations. A cybersecurity maturity model can help here, letting aviation organizations assess their current capabilities and build them up through defined stages.⁵⁴

The same logic applies to aircraft certification and continuing airworthiness. Indonesia should fold the RTCA and EUROCAE DO-326A family into its certification framework and require applicants to show that cyber risks were identified and adequately mitigated during aircraft design, modification, and maintenance, bringing cybersecurity into the certification process itself. Structured security requirements and data models for critical aviation systems give a more consistent basis for managing cyber risks across the aircraft lifecycle.⁵⁵

⁵³ Ahmed AbdelWahab ElMarady and Kamel Hussein Rahouma, "The Impact of COVID-19 on the Cybersecurity in Civil Aviation: Review and Analysis," in *2022 International Telecommunications Conference (ITC-Egypt)* (Cairo, Egypt: IEEE, 2022), 1–6, <https://doi.org/10.1109/ITC-Egypt55520.2022.9855692>.

⁵⁴ Ojaswini Malhotra *et al.*, "Cybersecurity Maturity Model Capability in Aviation and Railway Industry," in *ACIS 2022 - Australasian Conference on Information Systems, Proceedings* (Brisbane, Australia: Association for Information Systems, 2022), 1–8.

⁵⁵ Sergiy Gnatyuk, "Multilevel Unified Data Model for Critical Aviation Information Systems Cybersecurity," in *2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)* (Kyiv, Ukraine: IEEE, 2019), 242–47, <https://doi.org/10.1109/APUAVD47061.2019.8943833>.

4. Strengthening International Cybercrime Cooperation and Mutual Legal Assistance

Indonesia needs a stronger capacity for cross-border investigation and prosecution of aviation-related cybercrime. Adherence to the Budapest Convention on Cybercrime would provide it with a broader legal and institutional framework for obtaining electronic evidence, preserving data, and cooperating in investigations that cross into foreign jurisdictions. Accession to the Beijing Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation is worth considering, particularly to criminalize unlawful acts against civil aviation, including those enabled by technology.

None of this resolves the practical difficulties of cross-border investigations by itself. Indonesia should make fuller use of its existing Mutual Legal Assistance Treaties (MLATs) and negotiate new bilateral arrangements where they are missing, backed by clear domestic procedures for identifying the competent authority, preparing requests, preserving electronic evidence, and obtaining records from foreign service providers. Aviation cases raise this problem sharply, since the relevant evidence, server logs, passenger databases, flight information, communications records, and more, may sit across several jurisdictions at once. Faster channels for emergency preservation and evidence requests are also needed for incidents that directly threaten aviation safety. Cross-border cooperation matters because aviation infrastructure is interconnected: a cyber incident in one jurisdiction can involve systems, service providers, or evidence sitting somewhere else entirely.⁵⁶

5. Strengthening Aviation CSIRT, Information Sharing, and Technical Resilience

Indonesia should strengthen aviation-specific incident response by formally establishing a civil aviation Computer Security Incident Response Team (CSIRT), with clear responsibilities for detection, reporting, coordination, and recovery. This mechanism should connect to BSSN and existing national cybersecurity structures while keeping enough aviation-specific expertise of its own. Regular multi-stakeholder exercises involving the DGCA, BSSN, airlines, airports, and air

⁵⁶ Lykou, Iakovakis, and Gritzalis, “Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management.”

navigation service providers would help surface technical and institutional weaknesses before a major incident forces the issue. Information-sharing mechanisms should allow aviation entities to report vulnerabilities and incidents without unnecessary legal or commercial exposure; the Aviation Information Sharing and Analysis Center (A-ISAC) demonstrates what structured exchange between government and industry can look like. Better detection and response capabilities reduce dependence on reactive measures by catching threats earlier.⁵⁷

Technical resilience should extend to Global Navigation Satellite System (GNSS) vulnerabilities: regular assessments of jamming and spoofing risks in strategically important airspace, and contingency procedures for GNSS disruption that build in alternative navigation capabilities, clear reporting mechanisms, air traffic management procedures, and appropriate training. Research on aviation communication systems points the same way: cybersecurity belongs in the design of navigation and communication infrastructure, not bolted on as a separate concern.⁵⁸

6. Developing Cybersecurity Capacity and Formalising Public-Private Cooperation

Finally, Indonesia should pair workforce development with a formal public-private cooperation mechanism. The DGCA and other aviation authorities need specialized cybersecurity training for inspectors, safety personnel, air navigation personnel, and incident-response teams, and they need to recruit people who bring both aviation and cybersecurity expertise. Regular audits should check whether airlines, airports, and air navigation service providers maintain the required level of cyber protection; structured training and maturity-

⁵⁷ Anna Ilyenko *et al.*, “Module for Detecting and Analyzing Cyber Threats in Information and Communication Systems of Civil Aviation Facilities,” in *CEUR Workshop Proceedings*, ed. Sokolov V. *et al.*, vol. 3991 (Ukraine: CEUR-WS, 2025), 158–72.

⁵⁸ Nils Maurer and Corinna Schmitt, “Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- And Risk Analysis,” in *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, vol. 2019-April (Germany: IEEE, 2019), 1–13, <https://doi.org/10.1109/ICNSURV.2019.8735139>.

based assessment can move organizations from basic compliance toward continuous improvement.⁵⁹

Government institutions cannot manage cybersecurity alone, since much of aviation's digital infrastructure is operated or supported by private entities. Indonesia should establish a formal information-sharing mechanism among airlines, airports, air navigation service providers, aircraft and technology suppliers, and government agencies. A national aviation Information Sharing and Analysis Center (ISAC), or an equivalent mechanism linked to existing national structures, could provide a platform for sharing threat intelligence, vulnerabilities, and lessons learned from cyber incidents, with legal safeguards protecting information shared in good faith from unnecessary disclosure or liability. This kind of model strengthens collective situational awareness while recognizing the operational role private actors already play. Secure information-sharing technologies can also help build trust and confidentiality into public-private cybersecurity cooperation.⁶⁰

These reforms work as a connected programme, not as isolated regulatory fixes (see Figure 2). The immediate priority is a clear national direction, clarified institutional responsibilities, and the conversion of international standards into enforceable domestic requirements. International cooperation, incident response, technical resilience, workforce development, and industry participation can then operate within that framework, addressing the weaknesses identified in the compliance assessment while building on the strengths already present in Indonesia's aviation and national cybersecurity legislation.

⁵⁹ Ojaswini Malhotra *et al.*, "Cyber Security Maturity Model Capability at The Airports," in *ACIS 2021 - Australasian Conference on Information Systems, Proceedings* (Brisbane, Australia: Association for Information Systems, 2021), 1–11.

⁶⁰ Farah Hasin and Kazi Abu Taher, "Cyber Threat Mitigation of Impending ADS-B Based Air Traffic Management System Using Blockchain Technology," in *Advances in Intelligent Systems and Computing*, ed. Kaiser M.S. *et al.*, vol. 1309 (Dhaka, Bangladesh: Springer Science and Business Media Deutschland GmbH, 2021), 545–56, https://doi.org/10.1007/978-981-33-4673-4_44.

Conclusion

Indonesia has established a substantial legal and institutional basis for civil aviation cybersecurity through the Aviation Law, the ITE Law, Government Regulation No. 71 of 2019, Presidential Regulation No. 82 of 2022, BSSN Regulation No. 8 of 2020, and Ministerial Regulation No. 51 of 2020. The inclusion of cybersecurity in the National Aviation Safety Programme (NASP) 2024–2026 also shows a shift towards treating cyber risk as part of aviation safety and security governance. These developments demonstrate that Indonesia has moved beyond a purely technical understanding of aviation cybersecurity and has incorporated it into several areas of national regulation and institutional practice.

The assessment, however, shows that compliance with international standards is not uniform across the Indonesian framework. While some regulatory areas provide a clear basis for cybersecurity protection, others remain less developed in terms of institutional coordination, enforcement, and international cooperation. Indonesia should respond by developing a unified national aviation cybersecurity strategy, strengthening coordination between the Directorate General of Civil Aviation and BSSN, and integrating mandatory cyber risk management into aviation certification and oversight. Greater international cooperation, including consideration of accession to the Budapest Convention and Beijing Convention, should complement these domestic measures. Such reforms would provide a more coherent basis for protecting Indonesia's increasingly digital aviation sector.

This study is limited to the legal and institutional dimensions of civil aviation cybersecurity and relies mainly on normative analysis of primary and secondary sources. It does not examine the practical implementation of the framework through interviews, surveys, technical assessments, or other field-based evidence. Future research could therefore combine doctrinal analysis with empirical research involving aviation authorities, airlines, airports, air navigation service providers, cybersecurity agencies, and other relevant stakeholders. This would allow future studies to assess whether the legal standards identified in this

research are effectively implemented in practice and how the framework responds to emerging cyber threats.

References

- Abeyratne, Ruwantissa. "Cyber Terrorism and Aviation—National and International Responses." *Journal of Transportation Security* 4, no. 4 (December 2011): 337–49. <https://doi.org/10.1007/s12198-011-0074-3>.
- Ali, Muhammad, Yim-Fun Hu, Rameez Asif, and Jiang-Ping Li. "Security Risk Assessments and Countermeasures for Future Aeronautical Communication Network Architecture." In *Aviation Cybersecurity: Foundations, Principles, and Applications*, edited by Houbing Song, Abdullah Hopkinson, Tomaso De Cola, Tom Alexandrovich, and Dahai Liu, 141–80. Bradford, United Kingdom: Institution of Engineering and Technology, 2021.
- Beyond Machines. "Hacker Claims Breach of Indonesian Civil Aviation Authority." *BeyondMachines.Net*, June 2024.
- . "Indonesia Reports Government Data Center Hit by Ransomware." *BeyondMachines.Net*, June 2024.
- Bhakti, Agus, Arfin Sudirman, R Widya Setiabudi Sumadinata, and Arry Bainus. "State Defense Strategy in Facing Cyber Threats After Hacking Incidents on Government Institutions: A Case Study in Indonesia." *Journal of Human Security* 20, no. 1 (2024): 109–17. <https://doi.org/10.12924/johs2024.20116>.
- Blecken, Marvin, Harmut Hintze, and Ralf God. "Enabling Airworthiness Security by a Holistic Security Engineering Process at Various Aircraft Design Levels." In *ICAS Proceedings*, 1–12. Hamburg, Germany: International Council of the Aeronautical Sciences, 2024.
- Dwiaji, Lingga, Agung Mulyo Widodo, Gerry Firmansyah, and Budi Tjahyono. "Analysis of Knowledge Management Strategies for Handling Cyber Attacks with the Computer Security Incident Response Team (CSIRT) in the Indonesian Aviation Sector." *Asian Journal of Social and Humanities* 2, no. 6 (March 2024): 1341–53. <https://doi.org/10.59888/ajosh.v2i6.261>.
- Eleimat, Mahmaud, Omar Alharasees, and Arnold Oszi. "Advancements in Airport Security Technologies: A Patent Analysis." In *Proceedings of*

- 2024 1st Edition of the Mediterranean Smart Cities Conference, MSCC 2024*, edited by Dahmane A.B., Dahmane A.B., El Hibaoui A., and Essaaïdi M. Budapest, Hungary: Institute of Electrical and Electronics Engineers Inc., 2024. <https://doi.org/10.1109/MSCC62288.2024.10696990>.
- Elmarady, Ahmed Abdelwahab, and Kamel Rahouma. "Studying Cybersecurity in Civil Aviation, Including Developing and Applying Aviation Cybersecurity Risk Assessment." *IEEE Access* 9 (2021): 143997–16. <https://doi.org/10.1109/ACCESS.2021.3121230>.
- ElMarady, Ahmed AbdelWahab, and Kamel Hussein Rahouma. "The Impact of COVID-19 on the Cybersecurity in Civil Aviation: Review and Analysis." In *2022 International Telecommunications Conference (ITC-Egypt)*, 1–6. Cairo, Egypt: IEEE, 2022. <https://doi.org/10.1109/ITC-Egypt55520.2022.9855692>.
- Florido-Benítez, Lázaro. "The Types of Hackers and Cyberattacks in the Aviation Industry." *Journal of Transportation Security* 17, no. 1 (December 2024): 13. <https://doi.org/10.1007/s12198-024-00281-9>.
- Garcia, Anna Baron, Radu F. Babiceanu, and Remzi Seker. "Means of Compliance and Relation Between Security Standards in Airworthiness Engineering." In *Integrated Communications, Navigation and Surveillance Conference (ICNS)*, April:1–9. United States: IEEE, 2019. <https://doi.org/10.1109/ICNSURV.2019.8735318>.
- Gnatyuk, Sergiy. "Multilevel Unified Data Model for Critical Aviation Information Systems Cybersecurity." In *2019 IEEE 5th International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD)*, 242–47. Kyiv, Ukraine: IEEE, 2019. <https://doi.org/10.1109/APUAVD47061.2019.8943833>.
- Hadi Prayitno, Afen Sena, and Putra Wicaksono. "Building Digital and Sustainable Transportation of Indonesia Air Transport." *Journal of Information Technology, Computer Science and Electrical Engineering* 1, no. S1 (April 2024): 26–28. <https://doi.org/10.61306/jitcse.v1iS1.14>.
- Hasin, Farah, and Kazi Abu Taher. "Cyber Threat Mitigation of Impending ADS-B Based Air Traffic Management System Using Blockchain Technology." In *Advances in Intelligent Systems and Computing*, edited by Kaiser M.S., Bandyopadhyay A., Mahmud M., and Ray K.,

- 1309:545–56. Dhaka, Bangladesh: Springer Science and Business Media Deutschland GmbH, 2021. https://doi.org/10.1007/978-981-33-4673-4_44.
- Ilyenko, Anna, Sergiy Gnatyuk, Sergii Ilyenko, Olena Prokopenko, and Valentyna Teliushchenko. “Module for Detecting and Analyzing Cyber Threats in Information and Communication Systems of Civil Aviation Facilities.” In *CEUR Workshop Proceedings*, edited by Sokolov V., Ustimenko V., Radivilova T., and Nazarkevych M., 3991:158–72. Ukraine: CEUR-WS, 2025.
- Jeon, Sanghoon. “Improvement Measures for Aviation Security Policies and Security Management System Against Potential Cyber Threats In-Flight.” *The Journal of Korean Institute of Communications and Information Sciences* 48, no. 11 (November 2023): 1525–33. <https://doi.org/10.7840/kics.2023.48.11.1525>.
- Kandera, Branislav, Simon Holoda, Marian Jancik, and Lucia Melnikova. “Supply Chain Risks Assessment of Selected EUROCONTROL’s Surveillance Products.” In *2022 New Trends in Aviation Development (NTAD)*, edited by Andoga R. and Fozo L., 86–89. Žilina, Slovakia: IEEE, 2022. <https://doi.org/10.1109/NTAD57912.2022.10013524>.
- Klenka, Michal. “Aviation Cyber Security: Legal Aspects of Cyber Threats.” *Journal of Transportation Security* 14, no. 3–4 (December 2021): 177–95. <https://doi.org/10.1007/s12198-021-00232-8>.
- Kusumadewi, Puan Maharani, Kholis Roisah, Adya Paramita Prabandari, and Ramalina Ranaivo Mikea Manitra. “Analisis Standar Penerbangan Di Indonesia Berdasarkan Hukum Udara Internasional.” *Masalah-Masalah Hukum* 52, no. 3 (October 2024): 262–71. <https://doi.org/10.14710/mmh.52.3.2023.262-271>.
- Kutahya, Cengiz Kerem. “Securing the Digital Twin: Cybersecurity Strategies for Virtual Replicas in Aviation Management.” In *Utilizing Cybersecurity to Foster Business Innovation and Resiliency*, edited by Filiz Mizrak, 241–60. IGI Global, 2025. <https://doi.org/10.4018/979-8-3693-6417-8.ch011>.
- Longdong, Bryan Dennis. “Pengaturan Hukum Mengenai Pendaftaran Pesawat Udara Menurut Undang-Undang No 1 Tahun 2009 Tentang Penerbangan.” *Lex Privatum* 9, no. 3 (2021): 151–61.
- Lykou, Georgia, George Iakovakis, and Dimitris Gritzalis. “Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic

- Management.” In *Advanced Sciences and Technologies for Security Applications*, 245–60. Athens, Greece: Springer, 2019. https://doi.org/10.1007/978-3-030-00024-0_13.
- Maio, Francesco Di. “Centralized Security Governance for Air Navigation Services: Innovative Strategies to Confront Emerging Threats against Civil Aviation.” In *2014 International Carnahan Conference on Security Technology (ICCST)*, edited by Garzia F., Garzia F., Garzia F., Thomas G., and Pritchard D.A., 2014-Octob:1–6. Rome, Italy: IEEE, 2014. <https://doi.org/10.1109/CCST.2014.6986968>.
- Malhotra, Ojaswini, Sharmistha Dey, Ernest Foo, and Marde Helbig. “Cyber Security Maturity Model Capability at The Airports.” In *ACIS 2021 - Australasian Conference on Information Systems, Proceedings*, 1–11. Brisbane, Australia: Association for Information Systems, 2021.
- . “Cybersecurity Maturity Model Capability in Aviation and Railway Industry.” In *ACIS 2022 - Australasian Conference on Information Systems, Proceedings*, 1–8. Brisbane, Australia: Association for Information Systems, 2022.
- Malik, Haroon, Shahzaib Tahir, Hasan Tahir, Musfirah Ihtasham, and Fawad Khan. “A Homomorphic Approach for Security and Privacy Preservation of Smart Airports.” *Future Generation Computer Systems* 141 (April 2023): 500–513. <https://doi.org/10.1016/j.future.2022.12.005>.
- Manitra, Ramalina Ranaivo Mikea, Callista Putri Bourdeau, Kylatifa Ghaniya Aristi, and Muhammad Hazel Nailah Akbar. “Vanishing Universal Norms? Rethinking Erga Omnes in International Humanitarian Law Principles.” *Brawijaya Law Journal* 12, no. 2 (October 2025): 257–81. <https://doi.org/10.21776/ub.blj.2025.012.02.04>.
- Manitra, Ramalina Ranaivo Mikea, and Adya Paramita Prabandari. “AI in Hybrid Conflicts: Towards a Legal Framework for Cognitive Warfare.” *Cogent Social Sciences* 12, no. 1 (December 2026): 1–24. <https://doi.org/10.1080/23311886.2026.2681304>.
- Marketing-Interactive. “Details of 45m Batik Air Customers Leaked in 2019 Reportedly Resurface Online.” *Marketing-Interactive*, September 2022.
- Maurer, Nils, Thomas Graupl, Corinna Schmitt, and Gabi Dreö Rodosek. “PMAKE: Physical Unclonable Function-Based Mutual

- Authentication Key Exchange Scheme for Digital Aeronautical Communications.” In *Proceedings of the IM 2021 - 2021 IFIP/IEEE International Symposium on Integrated Network Management*, edited by Ahmed T., Festor O., Ghamri-Doudane Y., Kang J.-M., Schaeffer-Filho A.E., Lahmadi A., and Madeira E., 206–14. Wessling, Germany: Institute of Electrical and Electronics Engineers Inc., 2021.
- Maurer, Nils, and Corinna Schmitt. “Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- And Risk Analysis.” In *2019 Integrated Communications, Navigation and Surveillance Conference (ICNS)*, 2019-April:1–13. Germany: IEEE, 2019. <https://doi.org/10.1109/ICNSURV.2019.8735139>.
- Ministry of Transportation - Republic of Indonesia. “National Aviation Safety Plan 2024-2026.” ICAO, 2024.
- Mizrak, Filiz, and Gonca Reyhan Akkartal. “Prioritizing Cybersecurity Initiatives in Aviation: A Dematel-QSFS Methodology.” *Heliyon* 10, no. 16 (August 2024): e35487. <https://doi.org/10.1016/j.heliyon.2024.e35487>.
- Niraula, Madhu. “Cybersecurity and Interoperability of Aviation Safety Service Ecosystem.” In *Integrated Communication, Navigation and Surveillance Conference (ICNS)*, April:1–12. United States: IEEE, 2022. <https://doi.org/10.1109/ICNS54818.2022.9771482>.
- Nobles, Calvin. “Cyber Threats in Civil Aviation.” In *Security Solutions for Hyperconnectivity and the Internet of Things*, 272–301. United States: Navy, Independent Researcher, United States: IGI Global, 2017. <https://doi.org/10.4018/978-1-5225-0741-3.ch011>.
- . “Cyber Threats in Civil Aviation.” In *Emergency and Disaster Management*, 1–3:119–41. United States: IGI Global, 2019. <https://doi.org/10.4018/978-1-5225-6195-8.ch007>.
- Omolara, Abiodun Esther, Moatsum Alawida, and Oludare Isaac Abiodun. “Drone Cybersecurity Issues, Solutions, Trend Insights and Future Perspectives: A Survey.” *Neural Computing and Applications* 35, no. 31 (November 2023): 23063–101. <https://doi.org/10.1007/s00521-023-08857-7>.
- Oz, Tuncel. “Cybersecurity as a Strategic Lever for Innovation in Smart Aviation Ecosystems: A Review of Emerging Trends.” In *Utilizing Cybersecurity to Foster Business Innovation and Resiliency*, edited by Filiz Mizrak, 103–22. Istanbul Ticaret University, Turkey: IGI

- Global, 2025. <https://doi.org/10.4018/979-8-3693-6417-8.ch005>.
- Pearce, Hammond. "Counterfeits and Kill Switches." In *Futureshock*, 154–72. Boca Raton: CRC Press, 2025. <https://doi.org/10.1201/9781032702797-8>.
- Prabandari, Adya Paramita, and Ramalina Ranaivo Mikea Manitra. "Need of A Global Aviation Standard Compliance? Air Passenger Rights in Indonesia and Madagascar." *Jurnal Hukum IUS QUIA IUSTUM* 32, no. 1 (January 2025): 207–38. <https://doi.org/10.20885/iustum.vol32.iss1.art9>.
- Prabandari, Adya Paramita, and Efrema Ardratya Prakasita Puteri. "Standardization of Private Aircraft: Implications of Climate Change." In *IOP Conference Series: Earth and Environmental Science*, 1270:012028. Indonesia: Institute of Physics, 2023. <https://doi.org/10.1088/1755-1315/1270/1/012028>.
- Praditya, Editha, Syamsul Maarif, Yusuf Ali, Herlina Juni Risma Saragih, Rui Duarte, Firre An Suprpto, and Riant Nugroho. "National Cybersecurity Policy Analysis for Effective Decision-Making in the Age of Artificial Intelligence." *Journal of Human Security* 19, no. 2 (2023): 91–106. <https://doi.org/10.12924/johs2023.19020012>.
- Rakotoarisoa, Maminirina Fenitra, Heni Kurniasih, and Mikea Manitra Ramalina Ranaivo. "Advancing Regional Cooperation to Combat Marine Debris and Enhance Livelihoods in Indonesia: Translating Global Agendas into Local Action." *Marine Pollution Bulletin* 224 (March 2026): 119097. <https://doi.org/10.1016/j.marpolbul.2025.119097>.
- Republic of Indonesia. "Enhancing Cybersecurity in Civil Aviation through National and International Collaboration." ICAO, 2025.
- Sabillon, Regner, and Juan Ramon Bermejo Higuera. "The Importance of Cybersecurity Awareness Training in the Aviation Industry for Early Detection of Cyberthreats and Vulnerabilities." In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, edited by Degen H., Ntoa S., and Moallem A., 14059 LNCS:461–79. Logroño, Spain: Springer Science and Business Media Deutschland GmbH, 2023. https://doi.org/10.1007/978-3-031-48057-7_29.
- Saputra, Pradipta Nindyan, Arfin Sudirman, Obsatar Sinaga Sinaga, Wahyu Wardhana, and Nurul Hayana. "Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP)." *Central*

- European Journal of International and Security Studies* 13, no. 4 (2019): 104–20.
- Shah, Imdad Ali, N. Z. Jhanjhi, and Sarfraz Brohi. “Cybersecurity Issues and Challenges in Civil Aviation Security.” In *Cybersecurity in the Transportation Industry*, edited by Imdad Ali Shah and Noor Zaman Jhanjhi, 1–23. Kuala Lumpur, Malaysia: Wiley, 2024. <https://doi.org/10.1002/9781394204472.ch1>.
- Sheh, Raymond, Donald Harriss, and Karen Geappen. “Autonomous Aerial Drones Connecting Public Safety: Opportunities and Challenges for the Future.” In *AUVSI XPONENTIAL*, 1–26. United States: Association for Unmanned Vehicle Systems International, 2024.
- Shueb, Masladdin M., Chuyang Yang, and Xiaongdon Che. “An Innovative Design for Improving U.S. Airports’ Cybersecurity Based on Blockchain Technology.” In *2024 Systems and Information Engineering Design Symposium, SIEDS 2024*, 232–37. United States: Institute of Electrical and Electronics Engineers Inc., 2024. <https://doi.org/10.1109/SIEDS61124.2024.10534684>.
- Sitabuana, Tundjung Herning, Ramalina Ranaivo Mikea Manitra, Dixon Sanjaya, Ibra Fulenzi Amri, and Nethan. “The Urgency of Artificial Intelligence Code of Ethics.” *Indonesia Law Review* 14, no. 3 (December 2024): 101–23. <https://doi.org/10.15742/ilrev.v14n3.6>.
- Soesabdo, Hendronoto, Kurnia Toha, Ramalina Ranaivo Mikea Manitra, and Mevy Adine. “Global Competition Law Beyond Treaties: The Rise and Limits of Networks.” *Juridical Tribune-Review of Comparative & International Law* 16, no. 2 (2026): 204–23.
- Sudarto, Lidia Rina Dyahtaryani, and Nanang Trianto. “Analysis of Defense and Cyber Security in Airspace Management in Indonesia.” *LEX LAGUENS: Jurnal Kajian Hukum Dan Keadilan* 2, no. 2 (2024): 1–10.
- Taufik, A Fathan. “Indonesia’s Cyber Diplomacy Strategy as a Deterrence Means to Face the Threat in the Indo-Pacific Region.” *Journal of Physics: Conference Series* 1721, no. 1 (January 2021): 012048. <https://doi.org/10.1088/1742-6596/1721/1/012048>.
- Torens, Christoph. “Safety versus Security in Aviation, Comparing Do-178c with Security Standards.” In *ALAA Scitech 2020 Forum*, 1 PartF:1–12. Braunschweig, Germany: American Institute of Aeronautics and Astronautics Inc, AIAA, 2020.

<https://doi.org/10.2514/6.2020-0242>.

- Ukwandu, Elochukwu, Mohamed Amine Ben-Farah, Hanan Hindy, Miroslav Bures, Robert Atkinson, Christos Tachtatzis, Ivan Andonovic, and Xavier Bellekens. "Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends." *Information* 13, no. 3 (March 2022): 1–22. <https://doi.org/10.3390/info13030146>.
- Utari, Indah Sri, Diandra Preludio Ramada, Ubaidillah Kamal, Ratih Damayanti, and Nizamuddin Alias. "The Digital Sanctuary: Forging Legal And Ethical Frameworks For Interfaith Coexistence Online." *Contemporary Issues on Interfaith Law and Society* 4, no. 2 (2025). <https://doi.org/10.15294/ciils.v4i2.35309>.
- Wahidah, Baiq Farhatul, Rizkiati Khasanah, and Fadly Husain. "Anatomical Traits and Economic Potential of *Amorphophallus Variabilis* and Conservation Implications in Selo Arjuno Forest, Central Java, Indonesia." *Biodiversitas* 27, no. 2 (2026). <https://doi.org/10.13057/biodiv/d270213>.
- Weiland, LV, and G Wei. "Evaluating the Impact of NextGen's Air Traffic System on Aviation Security." In *MATEC Web of Conferences*, edited by Nader Asnafi, 189:10030. Embry Riddle Aeronautical University, United States: EDP Sciences, 2018. <https://doi.org/10.1051/matecconf/201818910030>.
- Wilis, Rakha, and Jackson Sidabutar. "How Can Gov-CSIRT Indonesia Maintain National Cybersecurity in the Future?" In *2024 16th International Conference on Information Technology and Electrical Engineering (ICITEE)*, 440–45. Bogor, Indonesia: IEEE, 2024. <https://doi.org/10.1109/ICITEE62483.2024.10808204>.

Acknowledgment

The authors would like to express their gratitude to the Faculty of Law, Universitas Diponegoro, and ASTA Research Center for their invaluable support in writing this paper.

Funding Information

This is funded by Faculty of Law, Universitas Diponegoro.

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement

None.