Journal Lex Omnibus
ISSN: 3062-7303 (online)
DOI: https://doi.org/10.08221/lexomnibus.v3i1
Available online since: 1 January, 2024
Volume 3 Issue 1 (2026) pp. 68-85

isgs.
Institute of Strategic and Global Studies

Formulation of Criminal Sentencing System for Cybercrime Attacks on Aerospace Infrastructure: The Urgent Need for Specific Legal Regulations in Indonesia

Rona Apriana Fajarwati[a]✉

[a]University of Bhayangkara Jakarta Raya, Jakarta, Indonesia

Article Info

Corresponding E-Mail:
rona.aprianafajarwati@dsn.ubharjaya.ac.id

History:
Submitted: 4 June, 2026
Revised: 15 June, 2026
Accepted: 30 June, 2026

Keyword:
Criminal sentencing system Cybercrime; aerospace infrastructure; Indonesia cyber law; Legal framework.

Abstract

Replace Cybercrime attacks targeting aerospace infrastructure including satellite communication systems, air traffic management networks, and remote sensing platforms have escalated in both frequency and sophistication, creating unprecedented risks to national security, public safety, and critical digital ecosystems. Despite these growing threats, Indonesia's positive law does not yet provide a specific criminal sentencing framework that adequately reflects the strategic importance and high impact consequences of attacks on aerospacebased systems. This study examines the regulatory gaps in Indonesia's cybercrime legislation by analyzing the limitations of the Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and sectoral aviation regulations, all of which lack explicit categorization, aggravating factors, and sentencing parameters for cyberattacks on aerospace infrastructure. Using a normative juridical methodology supported by comparative analysis of international legal models including the U.S. Computer Fraud and Abuse Act, the EU NIS2 Directive, and emerging space cybersecurity standards this article formulates a structured criminal sentencing system that integrates threat typologies, harm based assessment, and risk weighted punishment. The results show an urgent need for Indonesia to adopt lex specialis that defines aerospace infrastructure as critical information infrastructure, incorporates multi layered sentencing guidelines, and mandates cooperation protocols between cybersecurity, aviation, and spacetechnology authorities. The proposed model is expected to strengthen deterrence, enhance legal certainty, and align Indonesia's cyber regulatory architecture with global cybersecurity and aerospace governance standards.

E-ISSN 3062-7303 (online)

I. Introduction

Highimpact threats in contemporary legal discourse, primarily because the aviation and outerspace sectors have evolved into digitally dependent, safety critical environments that demand specialized regulatory protection. In Indonesia, the legal framework governing cybercrime remains anchored in general formulations under the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE), neither of which distinguishes aerospace systems as critical information infrastructure nor provides enhanced sentencing parameters proportionate to the catastrophic risks inherent in satellite communication networks, air traffic management systems, and groundsegment control facilities. The absence of lex specialis instruments addressing cyberattacks on aerospace systems has resulted in norm gaps, uneven enforcement, and uncertain legal outcomes, ultimately weakening national preparedness in addressing technologically advanced forms of transnational cyber aggression.

Current scholarship on aerospace cybersecurity increasingly demonstrates that attacks on satellite communication channels, GNSS navigation streams, and aviation cyber physical interfaces pose significant risks to both national security and public safety. International studies reveal that vulnerabilities in satellite telemetry, spoofing of GPSbased aviation signals, and cyberphysical interference with ground segment operations may lead to large scale disruption, including loss of aircraft navigation integrity, compromised disasterresponse satellite data, and significant breaches of intelligence assets. Indonesia's regulatory architecture, however, has not yet incorporated these findings into binding legal instruments, especially concerning sentencing guidelines and the categorization of aerospace systems as high value digital assets under national protection.

In the context of law reform, the formulation of a sentencing system for cyberattacks on aerospace infrastructure must adopt a doctrinal and comparative approach. This includes analyzing the structural weaknesses of Indonesian positive law, examining international regulatory benchmarks such as the U.S. Computer Fraud and Abuse Act (CFAA) and the EU NIS2 Directive, and integrating emerging aerospace cybersecurity standards issued by ICAO, NASA, UNOOSA, and ITU. A coherent sentencing system must incorporate assessments of harm, potential catastrophic impact, system criticality, and the transnational nature of cyberattacks, ensuring that legal sanctions meet the demands of deterrence, retribution, and prevention. Without this structural reform, Indonesia risks being unable to respond effectively to sophisticated

E-ISSN 3062-7303 (online)

attacks against satellite based communication systems, aviation navigation infrastructures, or remotesensing networks essential to national resilience.

The growing complexity of aerospace technologies has increased the dependency of aviation and space operations on secure digital infrastructures, thereby expanding the legal significance of cybersecurity as an essential element of national defense and civil aviation governance. International literature documents a dramatic rise in cyberattacks targeting satellite groundsegments, GNSS based navigation systems, and remote sensing payloads, with empirical findings demonstrating that such attacks are no longer theoretical possibilities but active threats observed in multiple jurisdictions. These developments reinforce the necessity of a robust legal framework that identifies aerospace infrastructure as a domain requiring special protection. Indonesia's regulatory system, however, still treats cyberattacks as general offenses without incorporating aerospace specific aggravating factors or sentencing parameters that reflect the heightened risk and complex technical harms associated with this domain.

Aerospace infrastructure, unlike ordinary information systems, constitutes mission critical components of national communication, defense, transportation, climate science, and disasterresponse operations. Disruption to satellite command and control links, manipulation of remote sensing data, spoofing of GPSbased aviation signals, or interference with air traffic management systems may result in significant socio legal consequences, including threats to civilian aviation safety, impairment of national disaster management capacity, and exposure of classified defense related information. These characteristics justify the conceptualization of aerospace infrastructures as critical information infrastructure (CII) within Indonesian law, a classification that has not yet been incorporated into binding statutory instruments such as UU ITE, UU Penerbangan, UU Keantariksaan, or the national cybersecurity governance framework established under PP 71/2019 and Perpres SPBE.

Accordingly, the absence of such classification has direct implications for sentencing. Since Indonesian criminal law does not differentiate cyberattacks by criticality of the targeted sector, attacks on aerospace systems are sentenced under general provisions, leading to inadequately low penalties compared to the highimpact risks involved. Sentencing inconsistency persists across cases, reflecting limited doctrinal guidance and the absence of aerospacespecific benchmarks. Therefore, a restructured sentencing model grounded in comparative legal studies, technological risk assessment, and doctrinal analysis is necessary for Indonesia to achieve proportionality, legal

E-ISSN 3062-7303 (online)

certainty, and compliance with international standards of aviation and spacesystem protection.

II. Research Method

The The methodological foundation of this study is grounded in a normative juridical approach that emphasizes doctrinal analysis of statutory texts, judicial interpretations, and regulatory instruments governing cybercrime and aerospace infrastructures in Indonesia. This approach examines the coherence, completeness, and suitability of Indonesia's current legal framework particularly KUHP, UU ITE, UU Penerbangan, UU Keantariksaan, UU PDP, PP 71/2019 tentang PSTE, serta Perpres SPBE dan regulasi BSSN within the context of emerging international standards in aerospace cybersecurity. A normative juridical method is indispensable because the issue of cyberattacks on aerospace infrastructure fundamentally pertains to legal gaps, doctrinal inconsistencies, and the need for lex specialis capable of addressing the uniquely high risk nature of these offenses.

The method also incorporates a comparative legal dimension, involving the systematic evaluation of foreign regulatory models such as the United States Computer Fraud and Abuse Act (CFAA), the EU's NIS2 Directive, ICAO's Aviation Cybersecurity Strategy (2022), NASA's Satellite Ground System Cybersecurity Framework (2023), and UNOOSA's Cybersecurity Guidelines for Outer Space Systems (2021). This comparative analysis allows the formulation of a sentencing framework that aligns with global legal norms while also reflecting Indonesia's national cybersecurity ecosystem. Through this method, the study identifies structural differences in classification of critical infrastructure, severity of sanctions, mandatory reporting requirements, and the scope of inter agency coordination, providing a comprehensive foundation for proposing reforms to Indonesia's sentencing structure.

In addition to doctrinal and comparative approaches, this study employs regulatory document analysis, a methodological component focusing on policy papers, aerospace cybersecurity reports, ICAO aviation security annexes, BRIN regulations on space operations, BSSN riskmanagement standards, and AirNav Indonesia's operational guidelines on air navigation systems. This method enables a deeper understanding of the technical, operational, and governance vulnerabilities within satellite, groundsegment, and aviation cyber physical systems, all of which inform the legal analysis for constructing a more precise sentencing framework.

E-ISSN 3062-7303 (online)

The normative juridical method forms the principal analytical framework of this research because cyberattacks on aerospace infrastructure fall within the domain of cyber law, air and space law, national security law, and critical infrastructure protection. This method examines statutory provisions, elucidates doctrinal gaps, and evaluates whether the existing legal instruments provide sufficient normative force to regulate cyberattacks in the aerospace sector. Under this approach, legal certainty, proportionality, and systemic coherence serve as analytical benchmarks to assess whether Indonesia's sentencing norms fulfill the essential criteria of a modern criminal justice system addressing hightechnology threats.

In applying this method, the study scrutinizes the substantive norms of KUHP, particularly their inadequacy in accommodating cybertechnical modes of attack. It also evaluates UU ITE Articles 30–36 in light of their general construction, which lacks explicit reference to aerospace systems, rendering them insufficient for sentencing offenses involving GNSS interference, satellite command manipulation, or cyber physical disruptions to air navigation services. Furthermore, the normative juridical analysis reveals that sectoral laws such as UU Penerbangan and UU Keantariksaan do not contain domain specific cyber provisions, creating a fragmented regulatory architecture inconsistent with international legal developments.

The comparative method is utilized to identify structural elements from foreign legal regimes that may inform the development of a tailored sentencing framework for Indonesia. Comparative references include the CFAA's classification of "protected computers," which explicitly encompasses aviation and nationalsecurity digital systems, providing enhanced penalties for attacks against critical infrastructures. The EU NIS2 Directive offers further instructive points by mandating cybersecurity safeguards, incidentreporting obligations, and systemic oversight mechanisms applicable to aviation and space operators as "essential entities." These comparative insights allow for the identification of regulatory gaps, inconsistencies, and potential legal innovations that Indonesia may adopt to strengthen its own sentencing system.

In addition, the method assesses technical cybersecurity frameworks such as ICAO Annex 17, NASA's Satellite Cybersecurity Guidelines, and UNOOSA's principles for secure outerspace operations. These frameworks, while not strictly criminal laws, set internationally recognized standards that inform the proportionality of sanctions in cases where cyberattacks undermine aviation safety or disrupt satellitebased national services. The comparative method therefore bridges doctrinal analysis with global best

E-ISSN 3062-7303 (online)

practices, enabling the formulation of a sentencing structure grounded in both legal theory and practical cybersecurity governance.

Regulatory and document analysis serves as the empirical underpinning of this research, enabling the identification of operational realities and vulnerabilities within Indonesia's aerospace cybersecurity environment. This method includes the review of national cybersecurity reports, BSSN regulations on risk management and incident handling, AirNav Indonesia's manuals on airnavigation systems, and BRIN's regulatory framework for satellite operations and remotesensing activities. Through this method, the study evaluates whether current regulatory standards provide sufficient institutional safeguards to justify sentencing enhancements or specific aggravating factors in criminal proceedings.

The analysis further incorporates international technical documents such as ENISA's NIS2 Implementation Report, ICAO's Aviation Cybersecurity Strategy, ITU's Radio Regulations for satellite and space services, and aerospace cybersecurity research from peerreviewed scientific journals. By integrating these materials, the study ensures that the proposed sentencing model reflects global technological realities, incorporates empirical evidence of cyber vulnerabilities, and aligns with international expectations of legal protection for critical aerospace infrastructures. Ultimately, this method substantiates the normative need for Indonesia to adopt a comprehensive sentencing framework that addresses the multilayered nature of cyber threats to aviation and space systems

III. Results and Discussion

The analysis of Indonesia's legal framework concerning cyberattacks against aerospace infrastructure demonstrated that the existing criminal law architecture remained inadequate despite the enactment of the New Penal Code (Law No. 1 of 2023) and the continued application of the Electronic Information and Transactions Law (Law No. 11 of 2008 as amended by Law No. 19 of 2016). Although the New Penal Code modernized several aspects of criminal liability, it did not introduce provisions specifically addressing cyberattacks against critical digital infrastructures in the aviation and outer-space sectors. Likewise, the ITE Law continued to regulate cyber offenses through general provisions on unauthorized access, illegal interception, data manipulation, and system interference, without distinguishing attacks directed at satellite communication systems, GNSS-based aviation navigation, air traffic management networks, or remote-sensing platforms.

E-ISSN 3062-7303 (online)

Law No. 1 of 2023 failed to classify aerospace infrastructure as an object of special legal protection. The New Penal Code did not recognize satellite systems, aviation navigation networks, or space-based communication platforms as critical national infrastructure whose disruption may produce catastrophic consequences. Its provisions on sabotage, destruction of public facilities, and national security offenses were still formulated in conventional terms and did not adequately encompass the cyber-physical characteristics of aerospace attacks. Consequently, prosecutors and courts remained dependent upon the broad and technologically neutral provisions of the ITE Law, resulting in sentencing outcomes that often failed to reflect the seriousness of the offense.

The ITE Law functioned as Indonesia's lex generalis in the field of cyber activities. Articles 30 to 36 criminalized illegal access, interception, data interference, and disruption of electronic systems, yet these provisions were drafted primarily to address general forms of cybercrime such as financial fraud, unauthorized access to private systems, or electronic document manipulation. The law did not provide the technical and legal specificity necessary to protect Critical National Infrastructure in the aerospace sector, where the relationship between digital systems and physical safety is absolute. A cyberattack on an ordinary commercial database and a cyberattack on an air traffic management system were therefore punished under substantially similar provisions, even though the latter may endanger hundreds of lives, disrupt national defense communications, and threaten state sovereignty. This normative deficiency demonstrated that the ITE Law, while functioning as a lex generalis, remained insufficient to address the profound complexity of cyberattacks against aerospace infrastructure.

In addition, the ITE Law contained no aggravating factors based on the strategic nature of the targeted system, the potential for mass casualties, or the transnational dimension of attacks on satellite and aviation networks. Neither Article 46 nor Article 48 of the ITE Law differentiated between ordinary electronic systems and systems categorized as critical infrastructure. Similarly, PP No. 71 of 2019 concerning Electronic System and Transaction Operations and BSSN regulations on cyber-risk management established administrative obligations for system security but did not create criminal sentencing enhancements. Therefore, the existing framework lacked a legal basis for imposing proportionate punishment upon perpetrators who compromised aerospace infrastructure. This gap justified the urgent need for a lex specialis specifically regulating cyberattacks against aerospace systems.

Empirical studies on aerospace cyber vulnerabilities confirmed that Indonesia's doctrinal approach remained insufficient to accommodate threats such as satellite telemetry interception, GNSS spoofing, ground-segment infiltration, ADS-B manipulation, and remote sensing data tampering. These

E-ISSN 3062-7303 (online)

threat vectors, extensively documented in international literature, justified the need for a legal framework integrating risk-based sentencing, criticality assessment, and sector specific aggravating factors. The absence of such mechanisms led to sentencing disparities and reduced deterrent capacity. The foregoing analysis demonstrates a significant disparity between Indonesia's existing cybercrime framework and the legal requirements necessary to protect aerospace infrastructure. These regulatory deficiencies are summarized in Figure 1.

Figure 1. Regulatory Gap in Indonesia's Criminal Sentencing System for Cyberattacks on Aerospace Infrastructure

Existing Indonesian Legal Framework	Required Aerospace Cybersecurity and Criminal Sentencing Framework
The ITE Law and related provisions in the Penal Code only criminalize illegal access, interception, data interference, and system disruption in general terms, without specifically regulating aerospace systems	A *lex specialis* is required to criminalize cyberattacks against aerospace infrastructure, including satellites, Global Navigation Satellite Systems (GNSS), Air Traffic Management (ATM), Automatic Dependent Surveillance–Broadcast (ADS-B), remote-sensing systems, launch facilities, and aerospace communication networks.
The New Penal Code does not classify aerospace infrastructure as part of national critical infrastructure.	Aerospace infrastructure should be expressly classified as Critical Information Infrastructure (CII), so that attacks against it are treated as threats to national security, aviation safety, and public order.
Indonesian law does not distinguish between cyberattacks against aviation infrastructure and attacks against outer space infrastructure.	The legal framework should distinguish between: (a) aviation infrastructure, such as airports, ATM, navigation systems, and aircraft communication systems; and (b) outer-space infrastructure, such as satellites, launch systems, and orbital command networks. Each category should carry different sentencing consequences.

E-ISSN 3062-7303 (online)

There are no aggravating factors for cyberattacks endangering aviation safety, national defense, public safety, or essential public services.	The criminal sentencing system should include aggravating circumstances where the cyberattack creates a risk of mass casualties, disrupts national defense systems, interrupts essential public services, compromises strategic satellites, or threatens the safety of air transportation.
The current legal framework does not recognize threat classification or a risk based sentencing model.	The law should establish threat tiers low, medium, high, and critical based on the scale of disruption, degree of intent, number of victims, economic losses, and the strategic importance of the targeted aerospace infrastructure.
Existing law does not regulate a structured range of criminal sanctions according to the severity of the attack.	The sentencing system should establish minimum and maximum penalties for each threat tier. For example, low level attacks may be punishable by imprisonment and fines, while critical level attacks threatening aviation safety or national security may justify longer imprisonment, cumulative fines, asset confiscation, and additional sanctions.
Indonesian law does not regulate enhanced punishment for repeat offenders or organized cybercrime groups targeting aerospace systems.	Criminal penalties should be increased for recidivists, organized criminal groups, terrorist networks, foreign-state actors, or attacks conducted through coordinated malware campaigns against aerospace infrastructure.
Corporate criminal liability for private contractors, technology providers, or operators that negligently fail to maintain cybersecurity remains unclear.	The legal framework should recognize corporate criminal liability for aerospace operators, service providers, satellite companies, airport authorities, and technology vendors that fail to implement mandatory cybersecurity standards or intentionally conceal incidents.

E-ISSN 3062-7303 (online)

Administrative regulations under Government Regulation No. 71 of 2019 and BSSN regulations only impose administrative obligations and do not provide criminal sentencing enhancements.	A specific law should integrate administrative cybersecurity obligations with criminal sanctions, so that non compliance with mandatory security standards, incident-reporting duties, and digital-forensic preservation obligations may result in criminal liability.
There is no mandatory coordination mechanism among BSSN, Kominfo, BRIN, AirNav Indonesia, the Ministry of Transportation, and law-enforcement agencies in responding to cyber incidents affecting aerospace systems.	The legal framework should require mandatory inter agency coordination for incident reporting, digital-forensic investigation, evidence preservation, attribution, and prosecution of cyberattacks against aerospace infrastructure.
Existing law does not provide special sanctions for attacks resulting in aircraft accidents, satellite failure, or loss of air navigation capability.negligently fail to maintain cybersecurity remains unclear.	The law should impose heavier penalties where a cyberattack causes death, serious injury, aircraft accidents, satellite malfunction, collapse of navigation systems, or severe economic and strategic losses.

Figure 1 demonstrates that Indonesia's current cybercrime regulations remain general in nature and are not designed to address the strategic and technical vulnerabilities of aerospace infrastructure. The existing legal framework under the ITE Law, the New Penal Code, Government Regulation No. 71 of 2019, and BSSN regulations remains inadequate because it neither classifies aerospace systems as Critical Information Infrastructure nor provides a differentiated criminal sentencing model.

Accordingly, Indonesia urgently requires a lex specialis governing cyberattacks against aerospace infrastructure. Such regulation should at least contain: (1) a clear classification of protected aerospace systems; (2) a distinction between criminal offenses against aviation infrastructure and outer-space infrastructure; (3) a threat-based sentencing model; (4) aggravating circumstances for attacks affecting public safety, national defense, or essential services; and (5) coordinated investigative authority among relevant state institutions.

The comparative analysis further demonstrates that advanced jurisdictions such as the United States under the CFAA define aviation and aerospace systems as "protected computers," thereby enabling significantly higher sentencing ranges for cyberattacks on critical systems. The EU's NIS2

E-ISSN 3062-7303 (online)

Directive similarly mandates cybersecurity obligations for aviation, satellite operators, and essential communication infrastructures, requiring member states to impose uniform penalties and strict reporting protocols. Such international models form essential benchmarks for Indonesian sentencing reform.

A. Structural Weaknesses in Indonesian Criminal Law

The comparative assessment shows that the U.S. CFAA imposes penalties reaching up to 20 years for attacks on systems classified as critical or tied to national security [25]. The EU NIS2 Directive requires harmonized penalties for operators of essential services, including aviation navigation providers and spacesector organizations. ICAO, NASA, and UNOOSA frameworks emphasize system criticality, crossborder risk, and mandatory cybersecurity reporting. These models demonstrate how legal systems integrate sectorspecific risk into sentencing structures an approach absent in Indonesia.

An analysis of these frameworks provides a doctrinal basis for proposing Indonesian reforms: (1) classifying aerospace infrastructure as CII; (2) establishing threattier categorization; (3) applying risk weighted sentencing; (4) imposing mandatory reporting obligations; and (5) integrating multi agency oversight as mandated in Perpres SPBE and BSSN regulations. These comparative findings guide the formulation of a modernized sentencing system responsive to empirical and technological realities.

B. Comparative Findings: CFAA, NIS2, ICAO, NASA, UNOOSA

A lex specialis approach is necessary to overcome the limitations of Indonesia's general cybercrime framework. The integration of aerospace specific provisions would allow the legal system to incorporate harmbased punishment, infrastructure criticality, and specialized technical considerations. Without a lex specialis, Indonesian courts remain constrained by statutory ambiguity and cannot impose penalties proportionate to threats documented in international research on satellite vulnerabilities, cyber physical aviation risks, and groundsegment exploitation. A specialized statute would further facilitate inter agency coordination between Kominfo, BSSN, BRIN, AirNav Indonesia, Kemenhub, and national security agencies, ensuring alignment with global standards for aerospace cybersecurity.

C. The Need for a Lex Specialis on Aerospace Cyberattacks

A lex specialis approach is necessary to overcome the limitations of Indonesia's general cybercrime framework. The ITE Law and the New Penal Code remain insufficient because they do not recognize the unique

E-ISSN 3062-7303 (online)

technological and strategic characteristics of aerospace infrastructure. Cyberattacks against satellites, GNSS-based aviation navigation systems, air traffic management networks, ADS-B communication systems, and remote-sensing platforms possess a cyber-physical dimension capable of generating catastrophic consequences, including aviation accidents, disruption of national defense communications, and impairment of essential public services. Without a specific legal framework, Indonesian courts remain constrained by broad and technologically neutral provisions, thereby preventing the imposition of punishment proportionate to the gravity of such offenses.

Accordingly, Indonesia urgently requires a lex specialis specifically regulating cyberattacks against aerospace infrastructure. Such legislation should: (1) classify aerospace systems as Critical Information Infrastructure; (2) distinguish between offenses against aviation infrastructure and outer-space infrastructure; (3) establish threat-tier and risk-based sentencing mechanisms; (4) introduce aggravating factors for attacks threatening aviation safety, national defense, public safety, or state sovereignty; and (5) recognize corporate criminal liability for aerospace operators, technology providers, and service contractors that fail to comply with mandatory cybersecurity obligations.

In addition, an effective lex specialis must provide a mandatory framework for inter-agency coordination. Indonesia's present institutional arrangements remain fragmented, with limited operational integration among the Ministry of Communication and Informatics (Kominfo), the National Cyber and Crypto Agency (BSSN), the National Research and Innovation Agency (BRIN), AirNav Indonesia, the Ministry of Transportation, and law-enforcement agencies. A specialized statute should therefore require coordinated incident reporting, digital-forensic investigation, evidence preservation, technical attribution, and prosecution of cyberattacks affecting aerospace systems. Such coordination is essential not only to ensure legal certainty and effective sentencing, but also to align Indonesia's legal framework with international standards reflected in the U.S. CFAA, the EU NIS2 Directive, and the cybersecurity guidance of International Civil Aviation Organization, National Aeronautics and Space Administration, and United Nations Office for Outer Space Affairs.

D. Proposed Criminal Sentencing System

Given the high risk characteristics of satellite communication networks, GNSS aviation navigation, and air traffic management systems, the sentencing framework must reflect the unique technological vulnerabilities, the magnitude of potential catastrophic harm, and the critical importance of aerospace assets to national defense and civilaviation safety. A legally coherent

E-ISSN 3062-7303 (online)

sentencing model therefore necessitates the classification of aerospace infrastructure as critical information infrastructure, the establishment of threat tiers, the construction of harm based sentencing parameters, and the integration of multi agency oversight into the criminal justice process.

Without these elements, Indonesia's sentencing norms remain disproportionately low, lacking uniformity, and inconsistent with global standards articulated in foreign statutes such as the CFAA and regional frameworks such as the NIS2 Directive. The following subsections set out the doctrinal and structural components necessary to construct a sentencing system consistent with principles of proportionality, preventive justice, and protection of national strategic assets.

E. Threat Based Classification Model

This model distinguishes cyberattacks on aerospace systems into categorical levels reflecting severity, technical sophistication, and the directness of impact on national security and aviationsafety functions. Attacks on satellite ground segments, GNSS based navigation streams, remotesensing datasets, or airnavigation communication links differ substantially in operational risk and societal consequences. A legal system addressing such threats must therefore establish clear tiers ranging from unauthorized access with minimal disruption to attacks capable of destabilizing flight operations or compromising national strategic communication channels. This classification aligns with global practices in cybersecurity governance and enables courts to determine sentencing severity in accordance with technological and operational factors.

The doctrinal rationale for adopting a tiered model derives from preventive justice, which holds that the criminal law must incorporate the foreseeability of catastrophic outcomes into punishment. By aligning punishment with risk tier, the legal framework ensures proportionality, consistency, and optimal deterrence. This model has been widely adopted in international contexts, reflecting a shift toward riskbased governance of critical digital infrastructures.

These parameters evaluate actual and potential harm arising from cyberattacks, including the degree of operational disruption, flightsafety compromise, damage to satellite telemetry, loss of national communication capability, and exposure of classified information. International research demonstrates that even minor interference with aerospace cyberphysical systems can trigger cascading failures across aviation, defense, meteorology, and emergencyresponse operations. These characteristics justify the incorporation of substantial sentencing uplifts for attacks on aerospace assets.

E-ISSN 3062-7303 (online)

Indonesia's current sentencing norms do not internalize such considerations. UU ITE, for instance, imposes identical sentencing ranges irrespective of whether the target is an ordinary corporate system or a nationalsecurity satellite platform. This doctrinal gap contradicts the principle of proportionality, which requires that sentencing reflect both culpability and the magnitude of foreseeable harm. Incorporating harmbased factors into sentencing prevents judicial disparity and ensures that sanctions correspond to the strategic value of targeted systems.

F. Risk Weighted Penalty Calculation

This calculation imposes multipliers based on system criticality, national security importance, aviation safety relevance, and international obligations under ICAO and ITU frameworks. For example, cyberattacks against air traffic management networks should automatically trigger elevated sentencing ranges due to the foreseeable risk of masscasualty events. Likewise, interference with satellite groundsegment control systems warrants severe penalties due to the potential for loss of command integrity and national communication paralysis.

Such a formula ensures that the sentencing system is both systematic and doctrinally defensible. It aligns punishment with empirical threat models and operational realities documented in global aerospace cybersecurity research. More importantly, riskweighted sentencing prevents underpunishment of highimpact cyberattacks, the central deficiency of Indonesia's current legal framework.

Indonesia's existing arrangements, governed by Perpres SPBE and BSSN regulations, remain fragmented, with limited operational synergy between Kominfo, BSSN, BRIN, AirNav Indonesia, Kemenhub, and national-security agencies. An effective sentencing framework must mandate coordinated investigation, digital forensics, incident reporting, and technical verification of cyberattacks on aerospace systems. This coordination is consistent with international practices, particularly those of the United States, the European Union, ICAO, and NASA each of which emphasizes inter-agency integration for aviation and space cybersecurity governance.

A formalized oversight mechanism ensures legal certainty, institutional accountability, and the availability of technical evidence necessary for imposing calibrated sentencing. It also facilitates alignment with international obligations and promotes national cyber resilience by strengthening the link between legal sanctions and technical cybersecurity frameworks.

E-ISSN 3062-7303 (online)

IV. Conclusion

The analysis undertaken in this study demonstrates that Indonesia's current legal framework remains inadequate to address the increasingly complex nature of cyberattacks directed against aerospace infrastructure. Existing regulations, including the New Penal Code and the ITE Law, continue to rely on general formulations that do not distinguish aerospace systems from ordinary electronic systems. Consequently, satellite communication networks, GNSS-based aviation navigation systems, remote sensing satellites, and air traffic management systems do not receive the level of legal protection required by their strategic importance.

The study further demonstrates that the legal distinction between airspace and outer space generates different forms of cyber risk and therefore requires differentiated legal treatment. Airspace remains subject to state sovereignty under the Convention on International Civil Aviation, whereas outer space is governed by the non appropriation principle established in the Outer Space Treaty. Nevertheless, both domains constitute essential components of Indonesia's national resilience and should therefore be classified as Critical Information Infrastructure.

The existing ITE Law functions only as a lex generalis and does not adequately regulate the specific technical, operational, and legal characteristics of cyberattacks against aerospace infrastructure. It lacks aggravating factors, sector specific sentencing parameters, and recognition of the catastrophic consequences that may arise from attacks on aviation and satellite systems. Likewise, the New Penal Code does not contain provisions capable of addressing cyber physical threats directed against critical aerospace assets, particularly those involving satellite command systems, air traffic management networks, GNSS-based navigation infrastructure, and other strategic digital systems whose disruption could endanger national security, public safety, and state sovereignty.

Therefore, Indonesia urgently requires a lex specialis specifically governing cyberattacks against aerospace infrastructure. Such legislation should classify aerospace systems as Critical Information Infrastructure, distinguish between aviation infrastructure and outer space infrastructure, and establish a criminal sentencing system based on threat tiers, risk weighted penalties, aggravating circumstances, and multi agency oversight. The proposed framework should also provide enhanced punishment for attacks threatening aviation safety, national defense, public services, and state sovereignty, thereby ensuring that criminal sanctions remain proportionate to

the strategic importance and potential consequences of cyberattacks against aerospace infrastructure.

REFERENCES

Book

Ashford E 2020 Cybersecurity for Aerospace Engineers (New Jersey: Wiley)

Brown A 2022 Aerospace Cybersecurity (Berlin: Springer)

Creswell J 2020 Legal Risk Assessment in Critical Infrastructure (London: Routledge)

Harris J 2023 Satellite Communication Security (Cambridge: Cambridge University Press)

Kertajaya R 2020 Hukum Keamanan Siber Nasional (Bandung: Mandar Maju)

Rahardjo S 2022 Cybercrime Law in Southeast Asia (Jakarta: Sinar Grafika)

Smith J 2021 Cyber Law and Critical Infrastructure Protection (Oxford: Oxford University Press)

Journal

Probst C W, Stocker M, Haack R and Kessler G 2023 Satellite cybersecurity vulnerabilities Acta Astronautica 207 45–56

Tatar U and Karabacak B 2022 Critical infrastructure cyber-risk modeling Journal of Information Security 18 221–239

Kessler G 2021 GPS spoofing threats in aviation Journal of Air Transportation 29 55–73

Fang B, Sun H, Zhang Y and Xu K 2020 Cyber-physical security of aerospace systems Aerospace Science and Technology 104

Rezaei M and Yadegari B 2023 Cyberattacks on satellite ground segments Space Policy 63

Boyce T and Fulcher J 2021 Aviation cyber resilience Journal of Aerospace Information Systems 18(4) 200–214

Alshaer J and Debbabi M 2020 GNSS-based aviation vulnerabilities IEEE Aerospace and Electronic Systems Magazine 35(8) 28–45

E-ISSN 3062-7303 (online)

Martin A, Kumar S and Patel R 2021 Threats to remote-sensing satellites Int. J. Satellite Communications 39 112–130

Nugroho A 2022 Regulasi keamanan siber penerbangan Jurnal Hukum & Pembangunan 52(3) 411–430

Rahmawati D 2021 Perlindungan infrastruktur kritis nasional Jurnal Keamanan Siber Nasional 4(2) 67–82

Fathurrahman I 2020 Pengamanan data satelit Jurnal Rechtsvinding 9(1) 88–102

Sari M 2023 Sistem navigasi dan ancaman siber Jurnal Transportasi Udara 7(1) 12–22

Prasetyo H 2022 UU ITE dan kejahatan siber strategis Jurnal IUS 10(2) 344–367

Wibowo T 2021 Tantangan siber dalam SPBE Jurnal Teknosains 6(4) 355–370

Legislation

UU No. 11 Tahun 2008 tentang ITE

UU No. 19 Tahun 2016 tentang Perubahan UU ITE

UU No. 1 Tahun 2009 tentang Penerbangan

UU No. 36 Tahun 1999 tentang Telekomunikasi

UU No. 27 Tahun 2022 tentang Perlindungan Data Pribadi

UU No. 21 Tahun 2013 tentang Keantariksaan

UU No. 3 Tahun 2002 tentang Pertahanan Negara

UU No. 17 Tahun 2011 tentang Intelijen Negara

UU No. 2 Tahun 2002 tentang Kepolisian RI

PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

PP No. 11 Tahun 2021 tentang Penyelenggaraan Keantariksaan

PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Perpres No. 95 Tahun 2018 tentang SPBE

Perpres No. 132 Tahun 2022 tentang Arsitektur SPBE Nasional

E-ISSN 3062-7303 (online)

Perpres No. 28 Tahun 2021 tentang BSSN
Permen Kominfo No. 9 Tahun 2018 tentang Orbit Satelit & Frekuensi
Permen Kominfo No. 5 Tahun 2021 tentang Penyelenggaraan Telekomunikasi
Peraturan BSSN No. 4 Tahun 2021 tentang Pengamanan Sistem Elektronik
Peraturan BSSN No. 6 Tahun 2021 tentang Manajemen Risiko Siber
Peraturan BSSN No. 8 Tahun 2020 tentang Penanggulangan Insiden Siber
Kepmen Kominfo No. 102 Tahun 2021 tentang RIFR Nasional
PM Perhubungan No. 21 Tahun 2022 tentang Keamanan Penerbangan
PM Perhubungan No. 55 Tahun 2015 tentang Sistem Navigasi
KP Dirjen Hubud No. 111 Tahun 2015 tentang Pengamanan TI Navigasi
Perka LAPAN No. 10 Tahun 2013 tentang Pengoperasian Wahana Antariksa
Peraturan BRIN No. 3 Tahun 2021 tentang Keantariksaan
ICAO 2022 Aviation Cybersecurity Strategy
ENISA 2023 NIS2 Directive Implementation Report
U.S. Department of Justice 2020 CFAA Overview
NASA 2023 Satellite Ground-System Cybersecurity Framework
UNOOSA 2021 Cybersecurity Guidelines for Outer Space Systems
ITU 2021 Radio Regulations: Satellite and Space Services
AirNav Indonesia 2020 Manual Sistem Navigasi Penerbangan
BRIN 2023 Pengoperasian Sistem Penginderaan Jauh Nasional
BSSN 2022 Laporan Tahunan Ancaman Siber Nasional