

Cyber Threats to Airport Infrastructure as a National Security Issue: A Legal Review from the Perspective of Sishankamrata in Indonesia

Arya Seto Sutopo¹, Retno Saraswati²

^{1,2}Master of Law, Faculty of Law, Diponegoro University, Semarang, Indonesia

ABSTRACT: The increasing dependence of airport infrastructure on digital technology has made it more vulnerable to cyber threats, posing significant challenges to Indonesia's national security. This study aims to analyze the patterns of cyber threats targeting airport infrastructure and examine the implementation of the *Sistem Pertahanan dan Keamanan Rakyat Semesta* (Sishankamrata) as a strategy to prevent and mitigate such threats. Using a normative juridical approach, this research examines relevant constitutional provisions, statutory regulations, and legal literature concerning national defense, security, and cybersecurity. The study finds that cyber threats, including cyberattacks, cybercrime, and cyberterrorism, have implications beyond operational disruptions, affecting economic stability, public trust, and national resilience. In this context, Sishankamrata provides an integrated framework that emphasizes coordination among government institutions, the private sector, and society in strengthening cybersecurity and protecting critical infrastructure. Therefore, enhancing legal harmonization, institutional cooperation, and cybersecurity capacity is essential to improve the resilience of airport infrastructure and support Indonesia's national security in responding to evolving cyber threats.

KEYWORDS: Cyber threats, airport infrastructure, national security, Sishankamrata, cybersecurity, Indonesia.

I. INTRODUCTION

Security is a fundamental function in the administration of the state and cannot be separated from an understanding of the state, the nation, and the people. The state is understood as an organization of power that possesses territory, a population, and a sovereign government, while the nation refers to a community that shares a common identity and aspirations. In this context, the people are the primary subjects of the state and form the basis of the legitimacy of state power. In Indonesia, this concept has been articulated since the nation's founding, affirming that the protection of the entire nation and all Indonesian citizens is the state's primary objective.

This formulation was subsequently enshrined in the 1945 Constitution of the Republic of Indonesia ("1945 Constitution") as the constitutional basis for the maintenance of national security. Over time, through a process of constitutional amendments documented in the Comprehensive Text of Amendments to the 1945 Constitution, Volumes I through X, the principles of the rule of law and democracy were strengthened, and the division of defense and security functions among state institutions was defined more clearly. This demonstrates that the concept of security in Indonesia is not static but evolves in response to the dynamics of the political system and the challenges of the times.

In this context, a distinction has emerged between the concepts of state security and national security. State security is oriented toward protecting the state's existence, such as its sovereignty and territorial integrity, whereas national security has a broader scope because it encompasses both military and non-military aspects, including political, economic, and social dimensions. The concept of national security is understood as a dynamic condition that ensures the survival of the nation and the state from various threats, both domestic and foreign (Hanita, 2020). This distinction is reflected in the legal framework, particularly Law No. 34 of 2004 on the Indonesian National Armed Forces ("TNI Law") and Law No. 2 of 2002 on the National Police of the Republic of Indonesia ("Polri Law"), which divide defense and security functions between the TNI and the Polri. However, the evolution of modern threats, which are multidimensional in nature, has caused the boundary between defense and security to become increasingly blurred, thus requiring a more integrated approach. Indonesia, which adheres to the Universal People's Defense and Security System (Sishankamrata), involves all components of the nation in safeguarding the country's defense and security.

Airports are a crucial strategic infrastructure because they integrate various interconnected systems that rely on digital technology. Cyber threats to airports not only result in operational disruptions and economic risks but can also escalate into broader security issues. In this context, these threats are inextricably linked to national security dynamics because disruptions to

Cyber Threats to Airport Infrastructure as a National Security Issue: A Legal Review from the Perspective of Sishankamrata in Indonesia

aviation infrastructure can affect the stability of the nation on a broader scale. Aviation policies, including the opening or closing of air routes, are often influenced by a country's diplomatic conditions and geopolitical interests. Political tensions between countries can result in restrictions or even the suspension of certain flights, thereby directly impacting human mobility, logistics distribution, international trade, and the tourism sector. Therefore, airport security should not be viewed merely as a technical or operational issue, but also as part of a nation's strategic interests in maintaining economic stability, defense, and national sovereignty.

This study aims to examine the patterns of cyber threats targeting airport infrastructure and to analyze the implementation of Sishankamrata as a legal and strategic framework for preventing and responding to such threats. By employing a normative juridical approach, this research contributes to the discussion on strengthening Indonesia's national cybersecurity governance through improved legal harmonization, institutional coordination, and multi-stakeholder collaboration in protecting critical infrastructure.

II. METHODS

A. *Patterns of Cyber Threats Targeting Airport Infrastructure and Their Implications for Indonesia's National Security System*

The distinction between the concepts of state security and national security reflects the evolution of Indonesia's security paradigm from a traditional state-centered approach to a more comprehensive framework that recognizes multidimensional threats. State security is fundamentally concerned with safeguarding the existence of the state, including its sovereignty, territorial integrity, constitutional order, and the safety of the nation, as mandated by the 1945 Constitution of the Republic of Indonesia. This traditional perspective primarily emphasizes military defense and the protection of territorial borders from external aggression. However, contemporary security challenges have transformed the meaning of security itself. National security has consequently developed into a broader concept encompassing military and non-military dimensions, including political stability, economic resilience, public welfare, environmental sustainability, technological development, and cybersecurity. As argued by Asshiddiqie (2019), national security should be understood as a dynamic condition in which the state is capable of protecting its national interests and ensuring the continuity of governance, economic activities, and public order against threats originating from both domestic and international sources. This conceptual shift is particularly significant because cyber threats against airport infrastructure no longer merely endanger state sovereignty in the conventional military sense but also threaten economic continuity, public safety, technological resilience, and the uninterrupted provision of essential public services. Consequently, airport cybersecurity should be analyzed within the broader framework of national security rather than solely as an issue of aviation safety.

Within this broader understanding of national security, cyberspace has emerged as a strategic domain comparable to land, sea, air, and outer space. The rapid digitalization of critical infrastructure has significantly increased dependence on interconnected information and communication technologies, while simultaneously expanding the attack surface available to malicious actors. Airports, as highly digitized transportation hubs integrating operational technology (OT), information technology (IT), and communication systems, have become particularly attractive targets. Modern airport operations rely extensively on digital systems to manage passenger processing, baggage handling, flight information displays, surveillance systems, biometric identification, access control, air traffic coordination, and communication with airlines and government agencies. Consequently, any disruption to these interconnected systems has the potential to interrupt not only airport operations but also national transportation networks and broader economic activities.

In the aviation context, cyber threats generally manifest in three principal forms: cyberattacks, cybercrime, and cyberterrorism, each possessing distinct characteristics, objectives, and implications. A cyberattack refers to any deliberate attempt to compromise the confidentiality, integrity, or availability of digital systems and information assets. Such attacks frequently employ techniques including malware infection, ransomware deployment, Distributed Denial-of-Service (DDoS) attacks, supply chain compromises, and exploitation of software vulnerabilities. Within airport environments, cyberattacks commonly target operational databases, airport management systems, passenger information systems, and communication networks, resulting in flight delays, service disruptions, operational paralysis, and substantial financial losses.

Cybercrime, by contrast, primarily focuses on obtaining financial gain through unlawful exploitation of digital technologies. It encompasses offenses such as unauthorized access (hacking), phishing, identity theft, online fraud, credential theft, payment system manipulation, and illegal trafficking of sensitive information. Airports are particularly vulnerable because they process enormous volumes of personal and financial data belonging to passengers, employees, airlines, immigration authorities, customs agencies, and commercial operators. Consequently, compromised airport databases may expose sensitive personal information, facilitate identity fraud, enable financial crimes, and undermine public confidence in digital aviation services.

Meanwhile, cyberterrorism represents a more severe category of cyber threat due to its political or ideological motivations. Unlike financially motivated cybercrime, cyberterrorism deliberately targets critical national infrastructure to create widespread fear, disrupt essential public services, and exert political pressure upon governments. In aviation, cyberterrorist activities may target Air Traffic Control (ATC) systems, airport operational centers, navigation infrastructure, or communication networks that support flight safety. Successful attacks against these systems could potentially result in flight cancellations, prolonged airport shutdowns, cascading failures across transportation networks, or even aviation accidents if safety-critical systems were compromised. As noted by Saman Iftikhar (2024), cyberterrorism seeks not merely to inflict economic damage but to destabilize society by undermining confidence in essential public infrastructure.

Recent developments indicate that cyber threats against airport infrastructure have become increasingly sophisticated and organized. Attackers no longer rely solely on direct system intrusions but frequently exploit vulnerabilities within supply chains, cloud services, third-party vendors, and human factors through social engineering techniques. Advanced Persistent Threats (APTs), often associated with state-sponsored actors or highly organized cybercriminal groups, are capable of infiltrating networks over extended periods without immediate detection. Such actors collect strategic intelligence, monitor operational activities, and establish persistent access before launching disruptive attacks. This evolution illustrates that airports are no longer merely victims of isolated cyber incidents but have become strategic targets within broader geopolitical competition and hybrid warfare strategies.

The multidimensional consequences of cyber threats against airport infrastructure extend far beyond technical disruptions. Socially, significant cyber incidents may erode public confidence in the safety and reliability of air transportation. Public trust constitutes an essential component of national resilience because aviation serves millions of passengers annually while facilitating mobility, tourism, emergency response, and governmental functions. A major cyber incident affecting airport operations may generate public anxiety, reduce confidence in digital public services, and trigger broader concerns regarding governmental capability to protect critical infrastructure.

Economically, cyberattacks against airports may produce substantial direct and indirect losses. Direct losses include operational downtime, flight cancellations, recovery expenses, regulatory penalties, compensation claims, and investments required to restore compromised systems. Indirect consequences include declining tourism revenues, disruptions to international trade, interruptions within logistics supply chains, reputational damage to airlines and airport operators, and diminished investor confidence. Since airports function as central nodes within national and global supply chains, prolonged disruptions may affect multiple economic sectors simultaneously, thereby reducing national economic productivity and competitiveness.

From a geopolitical perspective, cyber incidents targeting airport infrastructure may significantly influence international perceptions regarding a country's cybersecurity maturity and institutional resilience. Persistent cyber vulnerabilities could affect bilateral aviation cooperation, cross-border intelligence sharing, international investment decisions, and compliance with global aviation security standards established by international organizations. Furthermore, sophisticated cyberattacks conducted by foreign state-sponsored actors may constitute elements of hybrid warfare, wherein cyberspace is employed to weaken strategic infrastructure without engaging in conventional military confrontation. Such operations blur the distinction between peacetime competition and armed conflict, presenting significant legal and policy challenges for national security institutions.

The strategic importance of aviation infrastructure is further reinforced by its classification as part of a nation's Critical Information Infrastructure (CII). Airports support governmental mobility, defense logistics, disaster response, humanitarian operations, and international commerce. Consequently, cyber incidents affecting airport infrastructure should not be interpreted solely as operational or technical failures but rather as potential threats to national resilience and sovereignty. The increasing convergence between digital technologies and critical infrastructure means that disruptions within airport systems may generate cascading effects across transportation, finance, customs, immigration, defense, telecommunications, and emergency response sectors.

Empirical evidence demonstrates the growing significance of these threats. Studies indicate that approximately 65 percent of cybersecurity incidents within the aviation industry target airport infrastructure, while the remaining attacks focus primarily on airlines and associated service providers. This pattern reflects the concentration of critical digital assets and interconnected operational systems within airport environments. Furthermore, according to data published by Indonesia's National Cyber and Crypto Agency (Badan Siber dan Sandi Negara/BSSN), approximately 347 significant suspected cyber incidents were recorded throughout 2023, encompassing ransomware attacks, data breaches, Distributed Denial-of-Service (DDoS) attacks, website defacement, and various forms of unauthorized system intrusion. These incidents affected multiple strategic sectors, including government institutions and transportation services. During the same period, approximately 1.67 million personal data records were reportedly exposed, illustrating the continuing vulnerability of Indonesia's digital ecosystem, particularly within sectors that support essential public services (Ahdiat, 2024).

Cyber Threats to Airport Infrastructure as a National Security Issue: A Legal Review from the Perspective of Sishankamrata in Indonesia

These developments demonstrate that cyber threats targeting airport infrastructure possess implications extending well beyond the aviation sector itself. They threaten economic stability, compromise strategic national data, weaken public trust in governmental institutions, and expose vulnerabilities within critical national infrastructure. As digital transformation continues to accelerate across Indonesia's transportation sector, cybersecurity must therefore be regarded not merely as an information technology issue but as an integral component of national security policy.

Accordingly, strengthening cybersecurity governance within the aviation sector requires a comprehensive approach that integrates legal regulation, institutional coordination, technological resilience, international cooperation, and continuous capacity building. Such efforts should include the implementation of robust cybersecurity standards, risk-based security management, real-time threat intelligence sharing, incident response mechanisms, regular cybersecurity audits, workforce training, and enhanced cooperation between airport operators, airlines, government agencies, and international organizations. Only through a holistic and adaptive cybersecurity framework can Indonesia effectively protect its airport infrastructure, safeguard national sovereignty, and maintain the resilience of its national security system against increasingly complex cyber threats in the digital era.

B. The Sishankamrata Concept as a Strategy for Preventing Cyber Threats to Airport Infrastructure in Indonesia

The Universal People's Defense and Security System (Sishankamrata) is a constitutional framework unique to Indonesia, rooted in the historical experience of the struggle for independence and the founding principles of the nation. This concept is explicitly set forth in Article 30 of the 1945 Constitution of the Republic of Indonesia, which affirms that efforts toward national defense and security are carried out through a system that involves all citizens, territory, and other national resources in a comprehensive, integrated, focused, and sustainable manner. The idea of public involvement in the defense system has existed since the deliberations during the sessions of the BPUPKI and PPKI, which positioned the people as the primary foundation of the state's strength in facing threats, whether from within or abroad (Sekretariat Negara RI, 1998).

The Sishankamrata framework reflects a "total defense system" approach that integrates military and non-military dimensions into a single national security policy framework. This system not only emphasizes the physical aspects of defense, but also encompasses ideological, political, economic, social, and cultural dimensions as part of national resilience. Therefore, national defense is not understood in a narrow sense as solely a military domain, but rather as a collective responsibility of all components of the nation, carried out comprehensively. This is reinforced in various laws and regulations that affirm the division of roles among the main, reserve, and supporting components within the national defense system.

The Sishankamrata framework encompasses two main concepts that are interrelated yet have distinct characteristics: "defense" and "security." Both share a common ground in their fundamental objectives: protecting the existence of the state, upholding sovereignty, and ensuring national stability. These two terms fall within the spectrum of national security, where defense and security are two inseparable sides that nonetheless possess distinct functional roles (Asshiddiqie, 2019).

The concept of defense within Sishankamrata is generally oriented toward efforts to counter external threats, particularly those of a military nature, such as aggression by other nations, territorial violations, or other forms of armed threats. The approach employed in the context of defense is the use of force, with the Indonesian National Armed Forces (TNI) as the primary instrument. Defense is strategic, organized, and oriented toward war scenarios. In this context, national defense serves to safeguard the nation's sovereignty, territorial integrity, and the safety of the entire nation from external threats that could directly jeopardize the nation's existence.

In contrast, the concept of security is more oriented toward a country's internal conditions, which include maintaining public order, enforcing the law, and protecting the public from various forms of domestic disturbances, such as crime, social conflict, terrorism, and other non-traditional threats. The primary instrument in carrying out security functions is the Indonesian National Police (Polri). Security has a broader dimension because it encompasses not only physical aspects but also social aspects and the well-being of the public. Thus, security is not merely repressive in nature but also preventive and persuasive in maintaining social stability.

The fundamental difference between defense and security within the Sishankamrata framework lies in the nature of the threats, the approaches employed, and the institutional authorities responsible. Defense focuses on external threats using a military-oriented approach, whereas security focuses on internal threats using a legal and social approach. In practice, the line between the two is not always rigid, especially when facing contemporary threats such as terrorism, cyber threats, and transnational crime, which are borderless in nature. This situation requires strong coordination and synergy among agencies, without blurring the principle of separation of functions that forms the basis of institutional professionalism.

The implementation of Sishankamrata in preventing cyber threats also emphasizes the importance of strengthening human resources and collective awareness of digital security. Airport operators and all parties involved in aviation operations need to possess the capabilities and understanding of cybersecurity to minimize the risk of data breaches and system sabotage. Thus, the concept of Sishankamrata is not only understood as a conventional defense system, but also as a national strategy

Cyber Threats to Airport Infrastructure as a National Security Issue: A Legal Review from the Perspective of Sishankamrata in Indonesia

that adapts to technological developments and new forms of threats. Through cross-sectoral cooperation and the participation of all components of the nation, the protection of airport infrastructure in Indonesia can be achieved more effectively and sustainably (Sarjito et.al, 2024).

CONCLUSIONS

The dynamics between the concepts of “state security” and “national security,” as well as their relationship to the concepts of “defense” and “security” within the Sishankamrata framework, indicate that Indonesia’s security system is moving toward an increasingly comprehensive and multidimensional approach. This development requires a balance between policy integration to address complex modern threats and the need for clarity in the division of authority among institutions, particularly between the TNI and the Polri. Without an integrated and harmonious legal framework, potential overlaps in authority could hinder the effectiveness of national security operations. Therefore, strengthening regulations and institutional coordination is crucial to ensure that the national defense and security system is not only adaptive to evolving threats but also continues to uphold the principles of the rule of law, institutional professionalism, and the protection of the public as the primary objective of security operations.

REFERENCES

- 1) Asshiddiqie, J. (2019). Pengantar Ilmu Hukum Tata Negara. Jakarta: Rajawali Pers.
- 2) Budiardjo, M. (2008). Dasar-Dasar Ilmu Politik. Jakarta: Gramedia.
- 3) Hanita, M. (2020). Ketahanan Nasional: Teori, Adaptasi, Dan Strategi. Jakarta: UI Publishing.
- 4) Lembaga Ketahanan Nasional RI. (2021). Ketahanan Nasional. Jakarta: Lemhannas RI.
- 5) Sadjijono. (2020). Hukum Kepolisian Di Indonesia. Yogyakarta: LaksBang.
- 6) Sarjito, Ir Aris, Ir Susilo Adi Purwantoro, M. SE, Much Mualim, Ir Ari Pitoyo Sumarno, MM SAP, George Royke Deksin et al. Geodefense Konsep Pertahanan Masa Depan. Indonesia Emas Group, 2024.
- 7) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku I). Jakarta: Sekretariat Jenderal MPR RI.
- 8) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku II). Jakarta: Sekretariat Jenderal MPR RI.
- 9) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku III). Jakarta: Sekretariat Jenderal MPR RI.
- 10) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku IV). Jakarta: Sekretariat Jenderal MPR RI.
- 11) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku V). Jakarta: Sekretariat Jenderal MPR RI.
- 12) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku VI). Jakarta: Sekretariat Jenderal MPR RI.
- 13) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku VII). Jakarta: Sekretariat Jenderal MPR RI.
- 14) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku VIII). Jakarta: Sekretariat Jenderal MPR RI.
- 15) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku IX). Jakarta: Sekretariat Jenderal MPR RI.
- 16) Sekretariat Jenderal MPR RI. (2010). Naskah Komprehensif Perubahan UUD Negara Republik Indonesia Tahun 1945 (Buku X). Jakarta: Sekretariat Jenderal MPR RI.
- 17) Sekretariat Negara RI. (1998). Risalah Sidang BPUPKI Dan PPKI 28 Mei 1945–22 Agustus 1945. Jakarta: Sekretariat Negara RI.
- 18) Mardhani, D., et al. (2020). Keamanan Dan Pertahanan Dalam Studi Ketahanan Nasional Guna Mewujudkan Sistem Keamanan Nasional. Jurnal Pertahanan & Bela Negara, 10(3).



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non-Commercial 4.0 International (CC BY-NC 4.0)

(<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.