IJSSR
International Journal of Social Service and Research

Vol. 6, No. 3, March 2026
e-ISSN: 2807-8691 | p-ISSN: 2807-839X

Strategies for Improving the Performance of Cybersecurity Systems in Supporting the Defense of National Airspace Sovereignty through an Information Security Management System (*ISMS*) Approach at *Koopsudnas*

Rianto Lismara[1]*, Sri Yunanto[2], Usni Hasanudin[3], Asep Kurnia[4]
Universitas Muhammadiyah Jakarta, Indonesia[1,2,3]
Institut Teknologi Bandung, Indonesia[4]
Email: riantolismara10@gmail.com[1]*, sri.yunanto@umj.ac.id[2], usnihasanudin@gmail.com[3], asepkurnia_98@yahoo.com[4]

Keywords
cyber security; airspace sovereignty; *koopsudnas*; defense policy; information security management system.

Info Article
Accepted:
Revised:
Approved:

ABSTRACT
This research is motivated by the transformation of defense threats from conventional patterns to cyber threats that are asymmetric, cross-border, and strategically impactful on national air defense systems. The reliance of *Koopsudnas* on information systems has increased significantly in parallel with the digitization of command, control, communication, computers, intelligence, surveillance, and reconnaissance (*C4ISR*) functions. The main problem addressed in this study is how to formulate a strategy to enhance the performance of cybersecurity systems through the Information Security Management System (*ISMS*) approach in order to strengthen national air defense and airspace sovereignty. This research aims to analyze the existing condition of cybersecurity within *Koopsudnas*, identify the level of cybersecurity maturity based on the Cyber Security Maturity Instrument (*IKAS*), and develop strategic recommendations integrated with defense policy. The study employs a policy research approach with a case study design and qualitative descriptive analysis using the *Plan–Do–Check–Act (PDCA)* cycle. The findings indicate that, while the cybersecurity system at *Koopsudnas* has established organizational structures and security mechanisms, it still requires strengthening in governance, policy integration, risk management, human resource capacity development, as well as optimization of internal controls and *ISMS*-based auditing. The formulated strategy emphasizes the integration of *ISMS* into the national air defense system, the strengthening of regulatory frameworks and information security culture, and enhanced inter-agency synergy to build adaptive and sustainable cyber resilience. This study concludes that strengthening cybersecurity constitutes a strategic defense policy instrument for upholding and maintaining national airspace sovereignty in the digital era.

INTRODUCTION

Throughout 2024, there were 23 violations of national airspace within the National Air Operations Command (*Koopsudnas*), consisting of 14 cases in the Kosek IKN area, 1 case in Kosek I, 7 cases in Kosek II, and 1 case in Kosek III (*Koopsudnas*, 2025). The violation was

carried out by foreign military and civilian aircraft without diplomatic permission or *valid flight clearance* (Putri et al., 2023; Sumantri et al., 2023). The high number of violations shows that the challenge of enforcing national air sovereignty is still significant. This challenge is not only related to the operational aspects of air enforcement, but also greatly influenced by the reliability of surveillance support systems as well as air defense command and control systems (Snoddy, 2024). In the context of modern air defense, the entire process of air law enforcement from radar detection, presentation of air traffic situation data, threat level assessment, to the issuance of interception orders is highly dependent on cyber-based information systems and data communication networks (Putri et al., 2023).

Therefore, any form of interference, manipulation, or control of the system by unauthorized parties against the air defense cyber system has the potential to directly undermine the state's ability to respond to airspace violations quickly, precisely, and legally The link between airspace violations and cyber threats is increasingly evident with the detection of *botnet attacks* on the *Koopsudnas* network on March 3 and 6, 2025 which were monitored at the *Network Operation Center* (NOC) (Koopsudnas, 2025). The attack has the potential to disrupt the *availability* and integrity *of* the air defense information system.

The impact of cyber disturbances can be in the form of a decrease in the quality of understanding of operational situations (*situational awareness*) and a slowdown in the decision-making process of air operations (USAF Scientific Advisory Board, 2021). Under certain conditions, this kind of cyber disturbance can be used as an *enabler* for airspace violations, either to obscure the traces of violations, delay interception responses, or create political and legal ambiguity in national airspace (Koopsudnas, 2025).

In the context of modern defense politics, airspace sovereignty is not only interpreted as the ability to enforce geographical boundaries, but also as a form of state political control over cyberspace that supports the national air defense system (AIIA, 2025; BSSN, 2023). Mastery of the cybersecurity system is a form of actualization of state power in defending its sovereignty. Countries that are weak in the cybersecurity system have the potential to lose control of their strategic information and defense infrastructure, thus opening up opportunities for intervention, sabotage, and digital espionage by state and non-state actors (AIIA, 2025; BSSN, 2023). Thus, cyber power is a defense political instrument that functions to maintain the existence of the state in the midst of global competition that has now shifted to non-physical space (AIIA, 2025; BSSN, 2023).

For Indonesia, its strategic geographical position in international air crossings makes control of airspace a vital political and defense interest. *Koopsudnas*, as the main command of the air defense operations of the Indonesian Air Force, has a mandate to maintain the integrity of the national airspace from all forms of threats. In carrying out this function, *Koopsudnas* operates information technology-based systems such as *Transmission Data Air Situation (TDAS), Thales Raytheon Skykeeper (THALES),* and *Air Defence Net-Centric System (AIRNETS)* which are integrated into the national radar data communication network (TNI AU, 2024). However, systems that rely heavily on this technology are easy targets for cyberattacks aimed at weakening air defense capabilities (Putri et al., 2023; TNI AU, 2024). When the defense digital system is disrupted, the country's political sovereignty in airspace is threatened (AIIA, 2025; Kompas.id, 2025).

Therefore, strengthening the air defense cybersecurity system must be seen as a strategic and political step, not just an operational technicality. The implementation of the Information Security Management System (SMKI) based on SNI ISO/IEC 27001:2022 is an important instrument to ensure the confidentiality, integrity, and availability of defense information. This approach provides a measurable risk management audit and control mechanism (BSSN, 2023). The integration of SMKI with the Cyber Security Maturity Assessment Instrument (IKAS) from the State Cyber and Cryptography Agency (BSSN) allows an objective assessment of the readiness of the cybersecurity system within the *Koopsudnas* environment, as well as the basis for the formulation *of evidence-based improvement* strategies (BSSN, 2023; Ajhari, 2023).

From the perspective of defense political science, cybersecurity must be seen as part of the state *power projection* strategy in the airspace. The failure of the state to protect the cyber air defense system is tantamount to lowering the political legitimacy of its sovereignty. Therefore, a strategy to improve cyber security is needed that not only closes technical gaps, but also strengthens Indonesia's political position and sovereignty in global airspace. The strategy must include three main pillars: first, strengthening cyber defense regulation and political governance; second, improving human resource capabilities and air defense technology; and third, inter-agency synergy in building national cyber resilience (AIIA, 2025; BSSN, 2023; TNI AU, 2024).

Thus, the urgency of this research lies in the effort to formulate a strategy to improve cyber security in maintaining and maintaining national airspace sovereignty through the Information Security Management System (SMKI) approach within the *Koopsudnas*. This research confirms that air sovereignty is not only a military issue, but also a political issue of national defense that determines Indonesia's existence and prestige in the regional and global security arena. Through a measurable and integrated cybersecurity improvement strategy, *Koopsudnas* is expected to be able to strengthen the national air defense system and affirm Indonesia's political sovereignty in airspace in the era of cyber warfare and multipolar geopolitics.

Several previous studies have shown the importance of cybersecurity governance and the application of international standards in protecting strategic information systems. Research by Yoga, Maharani, and Maulana (2024) shows that the implementation of ISO/IEC 27001:2013 and COBIT 5 standards is able to identify the level of information system security capability, although weaknesses are still found in the aspects of documentation, risk management, and continuous evaluation mechanisms. Furthermore, Frangky and Sinaga (2024) emphasized that the implementation of ISO/IEC 27001:2022 is effective in improving information system security, but its success is greatly influenced by management commitment and a supportive organizational culture.

Meanwhile, Rizki (2022) revealed that the cyber defense system in Indonesia still faces various challenges, such as overlapping authority, limited human resources, and the lack of integrated cybersecurity policies nationally. In addition, Sucahyadi's (2024) research on cyber defense strategies in *Koopsudnas* shows that cyber security efforts still focus on technical operational aspects and have not been fully integrated with defense political policies. Based on these findings, it can be concluded that strengthening cybersecurity governance integrated with strategic policies is an important factor in supporting the protection of air defense systems and maintaining national airspace sovereignty.

Airspace sovereignty is a symbol of the country's political power that reflects the legitimacy, independence, and capacity of national defense. In the context of modern defense politics, such sovereignty is no longer determined only by conventional military power, but also by the state's ability to control, protect, and control defense cyberspace as a new strategic domain. Cyber attacks on air defense systems are not just a technological threat, but a political threat that has the potential to weaken the authority and authority of the state in upholding sovereignty in national airspace (AIIA, 2025; Political Violence at a Glance, 2022).

This condition requires a cyber defense political strategy that is able to ensure the integrity of the air defense information system and strengthen the state's position in national security governance. In this case, *Koopsudnas* has a central role as the implementer of air defense operations that must be able to adapt to the dynamics of asymmetric threats in the digital era (AIIA, 2025; BSSN, 2023). The strengthening of the *Koopsudnas* cyber security system is not only interpreted as an increase in technical capabilities, but also as a political strategy for national defense to maintain the sovereignty of Indonesia's airspace (TNI AU, 2024; Wikipedia, n.d.).

Based on this context, the formulation of the problem in this study is "How is the Strategy to Improve Cyber Security in Supporting the Defense and Sovereignty of National Airspace Through the Information Security Management System (SMKI) Approach in *Koopsudnas*?". To clarify the focus of the study, the formulation of the problem is elaborated into the following research questions: 1) What are the characteristics and forms of cyber security threats to Indonesia's air defense system that have the potential to interfere with the enforcement of national airspace sovereignty? 2) What is the existing condition of Indonesia's defense in dealing with cyber threats that have an impact on national airspace sovereignty? 3) What is the strategic position of *Koopsudnas* in the national air defense structure related to strengthening the cybersecurity system? 4) What is the strategy to improve cyber security in *Koopsudnas* in order to maintain and defend the sovereignty of national airspace?

This research aims to analyze and formulate defense strategies through improving cyber security at the National Air Operations Command (*Koopsudnas*) in order to maintain and defend the sovereignty of national airspace. This research begins with an analysis of the existing conditions of Indonesia's defense in dealing with cyber threats that have the potential to affect national air sovereignty, including a study of the importance of airspace sovereignty, national political interests, and existing cyber defense systems.

Furthermore, this study identifies and evaluates the strategic position of *Koopsudnas* in the national defense system, including the organizational structure of the TNI and TNI AU, the duties and functions of *Koopsudnas* as the Main Command of Operations and Development, and its role in maintaining cyber security through the support of Satkominfosiber with an Information Security Management System (SMKI) approach.

This research is expected to provide both theoretical and practical benefits. Theoretically, this research contributes to the development of defense science, especially in the study of cybersecurity, defense politics, and airspace sovereignty through the application of the Information Security Management System (SMKI) based on SNI ISO/IEC 27001:2022. Practically, the results of this research can be a reference for *Koopsudnas* in formulating strategies and policies to improve cyber security that are effective, integrated, and able to improve cyber risk management in the air defense environment. In addition, this research also

provides policy recommendations for the Ministry of Defense and the Indonesian Air Force in strengthening cybersecurity-based air defense systems to support the realization of Indonesian airspace sovereignty in the digital era.

METHOD

This study used a *policy research approach* with a descriptive-analytical nature, which aims to produce strategic policy recommendations in improving cybersecurity within the National Air Operations Command (*Koopsudnas*). The policy approach was chosen because the problems studied are not only technical, but are directly related to the formulation of defense strategies and the enforcement of national airspace sovereignty. This approach allows researchers to assess the gap between the existing condition of the *Koopsudnas* cybersecurity system and the Information Security Management System (SMKI) standard in accordance with SNI ISO/IEC 27001:2022 (BSN, 2023). This study adopts *the Plan–Do–Check–Action* (PDCA) cycle as applied in the framework of SMKI SNI ISO/IEC 27001:2022, with adjustments for the context of cyber defense policies.

Research Location

This research was conducted at the National Air Operations Command (*Koopsudnas*) as the object of a case study. The selection of the location is based on the strategic function of *Koopsudnas* in maintaining national airspace sovereignty through air defense operations, law enforcement, and technology-based communication and information system management. *Koopsudnas* is also the main organizer of cybersecurity operations carried out by Satkominfosiber, so it is relevant as a *research locus* related to the audit of the Information Security Management System (SMKI).

Research Time

This research was carried out in the period from July 2025 to February 2026 with a schedule that was systematically prepared to ensure the regularity and smooth implementation of each stage of the research. The initial stage begins with the preparation of a draft research proposal in July, which is then continued with the guidance and revision process until mid-October 2025. Furthermore, the proposal seminar will be held on August 14, 2025 as a forum to obtain input from supervisors and examiners. The data collection stage in the form of observation and interviews will be carried out from September 2025 to mid-January 2026, accompanied by a data analysis process carried out in parallel towards the end of January 2026. The final stage of research in the form of preparing research reports and preparing for the thesis exam is planned for February 2026.

Research Approach

This study uses a *policy research approach* with a qualitative descriptive nature , which aims to analyze and formulate a strategy to improve cyber security of *Koopsudnas* in maintaining and maintaining national airspace sovereignty. The policy approach was chosen because the focus of this research is not only on the technical aspects of cybersecurity, but also on the formulation of strategic defense policies oriented towards strengthening air sovereignty through the implementation of the Information Security Management System (SMKI) based on SNI ISO/IEC 27001:2022.

Types of Research

The type of research used is *a case study*, with the main object of study being the National Air Operations Command (*Koopsudnas*) as an institution that has direct responsibility for securing national airspace. Through this case study, the research seeks to examine in depth the *existing* conditions of cyber security, its conformity with SMKI standards, and formulate a measurable improvement strategy in accordance with the direction of national defense policy. This approach allows researchers to dig into empirical data, assess policy gaps, and generate relevant recommendations in the context of cybersecurity-based air defense.

Informant Determination Techniques

Research informants are determined through *purposive* sampling techniques, namely the deliberate selection of informants based on the relevance of roles, experience, and competencies to the research focus on *Koopsudnas* cyber security in maintaining the security and sovereignty of national airspace. The selected informants are key officials and personnel who have direct responsibility for the management, supervision, and policies of the cybersecurity system within the *Koopsudnas*, namely: 1) *Dansatkominfosiber Koopsudnas*, is in charge of the sustainability of the Cyber Security System in the *Koopsudnas* Environment. 2) *Pabandya Renops Skomlek Koopsudnas*, is in charge of the implementation of planning in the *Komlek* field. 3) *Kasihar* Satkominfosiber, which plays a direct role in the security, maintenance, and development of cybersecurity systems in the *Koopsudnas* environment. 4) *Kasiops Satkominfosiber Koopsudnas*, which plays a direct role in the operation of the cyber security system within the *Koopsudnas*.

The selection of the informants is expected to provide an empirical and strategic overview of the actual conditions, challenges, and policy directions of strengthening the *Koopsudnas* cybersecurity system in supporting the defense and sovereignty of national airspace.

Data Collection Techniques.

The data collection technique in this study was carried out with a descriptive qualitative approach, which aims to gain an in-depth understanding of the existing conditions, policies, and cybersecurity strategies within the National Air Operations Command (*Koopsudnas*). Data was collected through three main techniques, namely interviews, documentation studies, and observations.

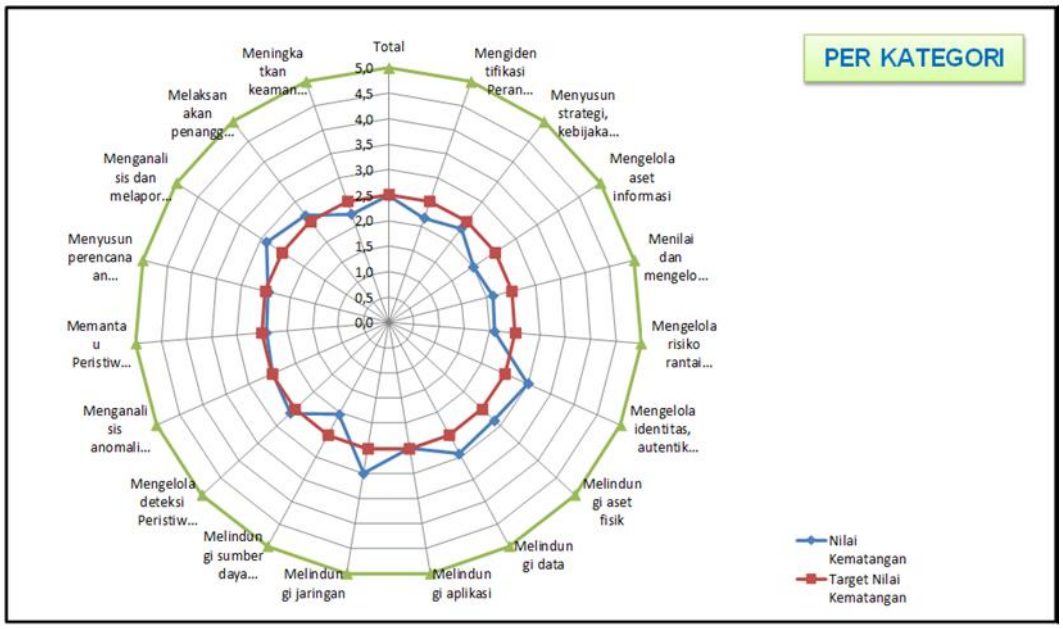
Data Analysis Techniques

This study uses an interactive qualitative data analysis model proposed by Matthew B. Miles and A. Michael Huberman, as described in Educational Research Methods (Sugiono, 2011). This model was chosen because it views data analysis as a process that takes place in a repetitive and interrelated manner, and is carried out simultaneously and continuously from the data collection stage to the drawing of final conclusions. In the context of research on strategies to improve the performance of the *Koopsudnas* cybersecurity system through the Information Security Management System (SMKI) approach, data analysis is carried out through several interrelated stages as follows: 1) Data Reduction. 2) Data Presentation. 3) Gap Analysis. 4) Cybersecurity *Maturity Assessment*. 5) Drawing Conclusions and Formulating Strategies.

RESULTS AND DISCUSSION

Results of Analysis of the Level of Cyber Security at *Koopsudnas*

The assessment of the level of cybersecurity maturity in *Koopsudnas* using IKAS analysis aims to evaluate the implementation of cybersecurity, identify risks, and formulate recommendations for improving cybersecurity in *Koopsudnas* so that it can increase public trust in cybersecurity in *Koopsudnas*. The results of the assessment of the level of cybersecurity maturity in *Koopsudnas* can be seen in Figure 1.



Source: Author's Research Results

Figure 1. Cybersecurity Maturity Level at *Koopsudnas*

The value of the cybersecurity maturity level in *Koopsudnas* is 2.49. This value is the value of the weighting results of 4 main domains, namely the identification domain 25%, the protection domain 30%, the detection domain 25%, and the countermeasures and recovery domain 20%. The identification domain consists of sub-domains identifying the roles and responsibilities of the organization; develop cybersecurity strategies, policies and procedures; managing information assets; assess and manage cybersecurity risks; as well as managing supply chain risks.

Protection domains consist of sub-domains managing identity, authentication and access control; protect physical assets; protect data; protect the application; protect the tissue; and protecting human resources. The detection domain consists of sub-domains managing the detection of cyber events; analyze anomalies and cyber events; and monitoring ongoing cyber events. The countermeasures and recovery domains consist of sub-domains of cyber incident countermeasures and recovery; analyze and report cyber incidents; implementing cyber incident response and recovery; and improve security after a cyber incident.

Based on Figure 1 Sub Domains that need improvement are identifying the roles and responsibilities of the organization; develop cybersecurity strategies, policies and procedures; managing information assets; assess and manage cybersecurity risks; and managing supply chain risks; protect the application; protecting human resources; analyze anomalies and cyber

events; monitoring ongoing cyber events; prepare cyber incident response and recovery planning; and improve security after a cyber incident. This is in accordance with the problems contained in *Koopsudnas*.

All areas contained in IKAS can be integrated into the clauses contained in SNI ISO/IEC 27001:2022. The IKAS assessment is compared to cybersecurity standards according to SNI ISO/IEC 27001:2022. Based on Figure 4.5, there are already several SNI ISO/IEC 27001:2022 clauses that have been met. The clauses that require improvement are clause 5.3 of the role, responsibilities and authority of the organization, clause 6.1 of actions to address risks and opportunities, clause 6.2 of information security objectives and planning to achieve them, clause 7 of support, clause 8 of operations, clause 9 of performance evaluation, and clause 10.1 of continuous improvement. This integration can provide control recommendations that can be applied for the sustainable development of cybersecurity systems.

The cybersecurity maturity level at *Koopsudnas* of 2.49 is included in the category of level 2 cybersecurity maturity level. Based on the guidelines for filling out the cybersecurity maturity assessment instrument, level 2 of the cyber security maturity level describes the conditions of cyber implementation in the repeated implementation stage, the implementation of cyber security already has organized procedures, the implementation of cyber security is informal, cyber security is carried out repeatedly but not yet consistent and not sustainable, risk management documents and control documents have been prepared and yet have not been determined (Directorate of Cyber Security Cybersecurity and Cryptography, 2024).

CONCLUSION

This study concludes that strengthening cybersecurity at *Koopsudnas* is a strategic necessity for safeguarding national airspace sovereignty amid multidomain threats, as evidenced by an *IKAS* maturity score of 2.49 (Level 2), which indicates that procedures exist but remain inconsistently implemented and unsustainable. Gap analysis highlights critical weaknesses in governance and policy integration, structured cyber risk management, human resource capacity, and continuous improvement especially in the identification and detection domains. Integrating the *IKAS* assessment with *SNI ISO/IEC 27001:2022* through the *Plan–Do–Check–Act (PDCA)* cycle offers a structured pathway to address these deficiencies.

The study emphasizes that cybersecurity functions not merely as a technical concern but as a strategic defense policy instrument influencing the state's ability to enforce airspace sovereignty, supported by strategies to strengthen regulations, align cybersecurity with air defense doctrine, enhance professional capacity, modernize infrastructure, and foster inter-agency collaboration. Future research should include comparative maturity assessments across all *Koopsudnas* air defense units, longitudinal studies on *ISMS*-based implementation over 3–5 years, cross-country analyses of air defense cybersecurity governance within ASEAN, development of a specialized cybersecurity competency framework for air defense personnel, and exploration of artificial intelligence and machine learning for proactive cyber threat detection.

REFERENCES

AIIA. (2025, November 6). Indonesia Needs Offensive Cyber Defence Posture. Australian Institute of International Affairs. https://www.internationalaffairs.org.au/australianoutlook/indonesia-needs-offensive-cyber-defence-posture/

AIIA. (2025, November 6). *Indonesia needs offensive cyber defence posture*. Australian Institute of International Affairs. https://www.internationalaffairs.org.au/australianoutlook/indonesia-needs-offensive-cyber-defence-posture/

Ajhari, A. A. (2023, March 19). *Cyber security maturity assessment BSSN for various stakeholders*. Medium. https://abdazzamajhari.medium.com/cyber-security-maturity-assessment-bssn-for-various-stakeholders-698ba0bed63d

Atrews, R. (2020). Cyberwarfare: Threats, security, attacks, and impact. *Journal of Information Warfare, 19*(4).

Atun, R., de Jongh, T., Secci, F., Ohiri, K., & Adeyi, O. (2018). Integration of targeted health interventions into health systems: A conceptual framework for analysis. *Health Policy and Planning, 33*(7), 727–737. https://doi.org/10.1093/heapol/czy040

BSSN. (2023). *BSSN enhances Indonesia's cybersecurity preparedness through strategic measures*. INTI Media. https://intimedia.id/read/bssn-enhances-indonesias-cybersecurity-preparedness-through-strategic-measures

BSSN. (n.d.). *Cyber security maturity (CSM)*. SNC.id. https://www.snc.id/product/detail/cyber-security-maturity-(csm)

Denning, D. E., & Strawser, P. (n.d.). *Applying air defense to the cyber domain*. Naval Postgraduate School.

Frangky, & Sinaga, R. (2024). The effectiveness of ISO/IEC 27001:2022 in improving information system security.

Frenk, J., Gómez-Dantés, O., & Knaul, F. M. (2019). The health system: Not just curative care. *The Lancet, 393*(10168), 2473–2476. https://doi.org/10.1016/S0140-6736(19)31209-0

Giles-Corti, B., Vernez-Moudon, A., Foster, S., et al. (2016). City planning and population health: A global challenge. *The Lancet, 388*(10062), 2912–2924. https://doi.org/10.1016/S0140-6736(16)30066-6

Kementerian Kesehatan Republik Indonesia. (2018). *Peraturan bersama tentang kabupaten/kota sehat*.

Koopsudnas. (2025). *Laporan pelanggaran wilayah udara nasional tahun 2024*.

Kruk, M. E., Gage, A. D., Arsenault, C., et al. (2018). High-quality health systems in the sustainable development goals era: Time for a revolution. *The Lancet Global Health, 6*(11), e1196–e1252. https://doi.org/10.1016/S2214-109X(18)30386-3

Kurniawan, A., Hidayana, I., & Susanti, H. (2020). Implementasi kabupaten/kota sehat di Indonesia: Tantangan dan peluang. *Jurnal Kesehatan Masyarakat, 16*(2), 123–134.

Levesque, J.-F., Harris, M. F., & Russell, G. (2019). Patient-centred access to health care. *International Journal for Equity in Health, 18*(1), 1–9. https://doi.org/10.1186/s12939-019-1035-8

Marmot, M., Allen, J., Goldblatt, P., et al. (2018). Health equity in England. *BMJ, 362*, k3646. https://doi.org/10.1136/bmj.k3646

Nieuwenhuijsen, M. J. (2021). Urban and transport planning and health. *Environment International, 158*, 106852. https://doi.org/10.1016/j.envint.2021.106852

Political Violence at a Glance. (2022, September 13). *The insidious political consequences of cyberattacks*. https://politicalviolenceataglance.org/2022/09/13/the-insidious-political-consequences-of-cyberattacks/

Putri, E., et al. (2023). Air defense strategy in improving security against airspace violations in Indonesia.

Rasanathan, K., Montesinos, E. V., Matheson, D., et al. (2017). Primary health care and intersectoral action. *The Lancet Planetary Health, 1*(9), e342–e349. https://doi.org/10.1016/S2542-5196(17)30160-2

Rizki, A. (2022). *Challenges in Indonesia's cyber defense system*.

Sallis, J. F., Cerin, E., Conway, T. L., et al. (2016). Physical activity in relation to urban environments. *The Lancet, 387*(10034), 2207–2217. https://doi.org/10.1016/S0140-6736(15)01284-2

Snoddy, D. (2024, January 5). *Air force cyber mission defense teams 2.0*. AFCEA International. https://www.afcea.org/signal-media/cyber-edge/air-force-cyber-mission-defense-teams-20-evolving-concept

Spicer, N., Agyepong, I. A., Ottersen, T., et al. (2020). Why fragmentation persists in global health. *Globalization and Health, 16*(1), 1–8. https://doi.org/10.1186/s12992-020-00588-2

Sucahyadi, B. (2024). *Cyber defense strategies in Koopsudnas*.

Sumantri, I. A., DAW, M., & Abu, S. (2023). Formation of Indonesian air defense strategy. *Journal of Politics, Security and International Relations, 1*(1).

TNI AU. (2024, September 10). *Indonesian air force sets cyber defence plans for next 20 years*. BERNAMA. https://bernama.com/en/news.php?id=2349520

USAF Scientific Advisory Board. (2021, June 8). *Cyber situational awareness abstract*.

Vlahov, D., Freudenberg, N., Proietti, F., et al. (2017). Urban health. *Annual Review of Public Health, 38*, 355–374. https://doi.org/10.1146/annurev-publhealth-031816-044216

Yoga, Maharani, & Maulana. (2024). Implementation of ISO/IEC 27001:2013 and COBIT 5 for information system security capability.