Digital Rights and Human Security: The Role of BSSN-KISA Collaboration in Protecting the Digital Rights of Indonesian Citizens

Rijal Aditia[1], Diyah Pitaloka Rizki[2]
Faculty of Social and Political Sciences, International Relations, Al-Ghifari University, Bandung, Indonesia
Email:

crewrizal009@gmail.com, diyahpitaloka801@gmail.com

ABSTRACT

The digitalization era has presented challenges in protecting Indonesian citizens' digital rights. This study analyzes the role of BSSN-KISA bilateral cooperation in protecting digital rights through human security approach. Using qualitative case study method, the research evaluates cooperation impact since 2022. Findings show cooperation has significantly contributed to personal data protection, cyber crime prevention (detection rate increased from 65% to 82%), digital literacy enhancement (2 million citizens), and critical infrastructure protection (40% downtime reduction). Indonesia's cyber resilience index improved from ranking 64 to 41 globally. Challenges include inter-agency coordination, budget limitations (0.08% GDP), and technological gaps. The study recommends strengthening regulatory framework, institutional strengthening, and multi-stakeholder engagement to optimize human security in digital era.

Keywords: *Digital rights, Human security, Cyber security, BSSN-KISA, Bilateral cooperation*

INTRODUCTION

1.1 Background

The ongoing digital transformation driven by the Indonesian government requires reliable and secure infrastructure to safeguard data and protect citizens' digital rights. BSSN emphasizes that cybersecurity serves as one of the key foundations for the successful implementation of the digital transformation agenda, particularly within the framework of Indonesia's G20 presidency (Ayu, 2022). The rapid pace of digitalization has triggered a surge in cyberattacks, posing threats to data confidentiality and citizens' digital rights. Incidents such as ransomware that locks government data and leaks of personal information highlight the urgent need to strengthen digital protection systems (Center, 2022). In an effort to strengthen national cybersecurity capabilities, BSSN has established a strategic partnership with the Korea Internet & Security Agency (KISA) of South Korea. The cooperation agreement between BSSN and KISA was officially signed on July 21, 2022, in Yogyakarta. This collaboration covers a wide range of initiatives, including the enhancement of human resource capacity, the transfer of knowledge and technological expertise, as well as the development of best practices in risk management and cyber incident response. The partnership is expected to reinforce Indonesia's digital resilience in addressing increasingly complex cyber threats (csirt, 2022).

This collaboration holds significant potential to strengthen citizens' digital rights, including the right to privacy, data security, access to information, and protection from potential digital violations. Enhancing national cybersecurity resilience will ensure the digital safety of citizens, in line with the principles of human security, which emphasize safeguarding individuals from various threats, including those in the digital realm. Although considerable progress has been made, major challenges remain, such as the need for more effective inter-agency coordination, the development of independent regulations, and stronger synergy among stakeholders. Therefore, continuous evaluation, governance reinforcement, adoption of best practices, and integration of national cybersecurity policies into the digital rights framework are crucial steps to ensure comprehensive and sustainable digital protection for the public. Indonesia, as a country with a rapidly growing number of internet users, faces significant challenges in safeguarding information security and protecting the personal data of its citizens. With widespread internet penetration, citizens increasingly rely on digital services for daily activities, ranging from online banking and e-learning to interactions with government services. This widespread digital dependence simultaneously creates opportunities for cybercriminals to carry out attacks such as data theft, malware, phishing, ransomware, and misuse of information, which can harm both individuals and institutions.

Cybercrime and digital threats today are transnational in nature, meaning attacks originating from abroad can target Indonesia's digital systems, with impacts that extend beyond technical issues to social, economic, and political consequences. Therefore, cybersecurity protection cannot rely solely on national strategies; a collaborative approach involving international cooperation is essential for sharing information, technology, best practices, and global cybersecurity standards. In this context, the strategic partnership between Indonesia's National Cyber and Crypto Agency (BSSN) and the Korea Internet & Security Agency (KISA) is of critical importance. This collaboration not only focuses on strengthening the national cybersecurity defense system through human resource development and technology transfer but also plays a role in establishing regulations, standards, and digital security protocols aligned with international best practices. Through these initiatives, Indonesia can enhance its digital resilience, improve protection of citizens' digital rights, and strengthen public trust in the national digital ecosystem, while affirming its position as a proactive member of the global community in addressing transnational cyber threats (antara, 2022).

1.2 Research Question

1. How does the collaboration between BSSN and KISA contribute to strengthening the protection of digital rights for Indonesian citizens?
2. How does the implementation of Indonesia's Personal Data Protection Law (UU PDP) affect the safeguarding of citizens' digital rights?
3. To what extent does the BSSN-KISA collaboration impact the enhancement of national cybersecurity resilience and the digital security of Indonesian society?

LITERATURE REVIEW

2.1 Theory of Internasional Relation

International relations, as a complex academic discipline, requires a deep understanding of the various facts and dynamics that shape the global order. Theories in this field serve as frameworks for describing, analyzing, and even predicting future events. Facts in international relations encompass a wide range of aspects, including interactions between states, global power dynamics, international cooperation, armed conflicts, cross-border trade, and global issues such as climate change and sustainable development. Without a solid theoretical foundation, these facts risk becoming fragmented information lacking clear direction or meaningful context (Dugis, 2016). According to Mochtar Mas'oed, international relations constitute a highly complex network of interactions because they involve sovereign states. This level of complexity requires mechanisms that are more sophisticated than those used in interactions between groups. This statement emphasizes that interactions among states in international relations demand a more advanced and intricate approach, given that each entity possesses its own sovereignty and distinct national interests (Humaira, 2023).

With the rapid development of the globalization era, various conveniences have emerged alongside the increasing interconnectedness of countries. Geographical barriers are no longer the main obstacle, as digital media and the internet allow individuals to connect and interact with people from all corners of the world. This phenomenon creates a reality where physical limitations no longer restrict communication and information exchange, enabling cross-cultural and cross-national interactions to develop more dynamically. The primary goal of International Relations (IR) involves detailed efforts to maintain global peace and security. Additionally, IR aims to enhance cooperation among countries across various sectors, including political, economic, and socio-cultural domains. In the political sphere, IR involves states in the establishment and maintenance of diplomatic relations as well as active participation in international negotiations, focusing on achieving universal objectives such as peace, conflict resolution, and the protection of human rights. In the economic domain, IR encourages countries to engage in international trade, cross-border investment, and cooperation in financial and development sectors, aiming to create a sustainable and mutually beneficial global economic framework. Meanwhile, in the socio-cultural aspect, IR promotes cultural exchange, tourism development, and scientific collaboration to strengthen mutual understanding and tolerance among nations. These efforts foster a harmonious climate among global communities and enrich cultural diversity at the international level (News, 2023).

2.2 Theory of Neoliberalism

From a neoliberal perspective, a country's sensitivity to its relative achievements how it assesses its successes or failures compared to other states is heavily influenced by its perceptions of the actions and capabilities of other countries. Within this framework, capabilities are considered significant only to the extent that they affect a state’s intentions and objectives. Furthermore, neoliberals emphasize the crucial role of international institutions and regimes in facilitating cooperation among states. These institutions and regimes serve as mechanisms for enforcing principles, norms, rules, and decision-making procedures, thereby enabling more effective and consistent interstate interaction and collaboration. Additionally, this approach highlights that international institutions not only reduce uncertainty and risk in state relations but also help create an environment that fosters stability, trust, and global integration (Dugis, 2016).

Neoliberalism theory is highly relevant for research on Digital Rights and Human Security: The Role of BSSN-KISA Cooperation in Protecting the Digital Rights of Indonesian Citizens, as this approach emphasizes the importance of international collaboration and private sector involvement in addressing global challenges, including cyber threats. By applying the neoliberal framework, this study can explore how BSSN and KISA cooperate to strengthen cybersecurity capabilities through policies aligned with open market principles, technological innovation, and cross-border collaboration. Furthermore, this approach allows for analysis of how such cooperation not only enhances digital security and resilience but also promotes the adoption of international best practices, knowledge exchange, and the creation of a safer and more sustainable cyber ecosystem for Indonesian society.

2.3 Theory of Human Security

The theory of *human security* was first introduced by the United Nations Development Programme (UNDP) in the 1994 Human Development Report. According to UNDP, *human security* refers to the protection of the core aspects of human life from serious and widespread threats, while simultaneously enhancing individual freedom and fulfillment. This concept emphasizes that the primary focus should be on the security of individuals, rather than solely on the security of the state. Threats to *human security* include fears, such as violence, conflict, and human rights violations, as well as deprivations, such as poverty, hunger, disease, and social inequality. The *human security* approach proposes two main strategies: protection and empowerment. Protection aims to reduce or eliminate threats to individuals, while empowerment focuses on enhancing the capacity of individuals and communities to face challenges and make informed decisions for their well-being. Both strategies complement each other and are essential for achieving comprehensive human security.

In the context of Indonesia, the application of *human security* can be seen in efforts to protect citizens' digital rights. With the rise of cyber threats, the state needs to expand its focus beyond traditional national security to include the protection of individuals from digital threats that could disrupt their daily lives. The collaboration between Indonesia's National Cyber and Encryption Agency (BSSN) and the Korea Internet & Security Agency (KISA) serves as a concrete example of applying the principles of *human security* in the digital realm (UNDP, 1994).

In the context of this study, the theory of Human Security is highly relevant because it emphasizes the importance of protecting individuals as the central focus of security policies, rather than focusing solely on state security. This theory expands the concept of security from merely safeguarding territorial integrity and national sovereignty to protecting the fundamental rights of citizens across various dimensions, including economic security, food security, health, environmental protection, as well as personal and community safety. Therefore, Human Security provides an appropriate conceptual framework for understanding how citizens' digital rights such as privacy, personal data protection, and access to digital services must be comprehensively safeguarded.

The collaboration between Indonesia's National Cyber and Crypto Agency (BSSN) and the Korea Internet & Security Agency (KISA) can be seen as an implementation of Human Security principles in the digital domain. Through this partnership, strategic measures are undertaken to ensure freedom from fear in cyberspace, such as preventing cyber threats, data breaches, and digital attacks that could harm citizens. In addition, this cooperation supports freedom from want in the digital realm by developing human resource capacity, providing cybersecurity technology and infrastructure, and formulating policies and regulations that effectively protect individual digital rights. Moreover, Human Security emphasizes the connection between individual protection and broader socio-political stability. By strengthening citizens' digital security, the BSSN-KISA collaboration not only safeguards individual rights but also enhances public trust in government digital systems and services. This, in turn, contributes to the creation of a safe, sustainable, and inclusive digital ecosystem, which is a core objective of the Human Security approach.

Thus, the theory of Human Security not only provides a theoretical foundation for this study but also helps analyze the role of international cooperation in the context of cybersecurity, digital rights protection, and human capacity building elements that are all crucial for ensuring the welfare and security of citizens in the digital era.

RESEARCH METHODOLOGY

Metode penelitian adalah pendekatan ilmiah yang digunakan untuk mengumpulkan data dengan tujuan tertentu serta memperoleh manfaat yang diinginkan. Dalam pelaksanaan penelitian, peneliti perlu menerapkan langkah-langkah atau strategi tertentu untuk mengatasi hambatan yang mungkin muncul dan mencapai tujuan penelitian yang telah ditetapkan. Adanya masalah dalam penelitian menuntut pendekatan yang sistematis dan terstruktur agar hasil yang diperoleh valid dan bermakna. Dalam konteks ini, pentingnya pemilihan metode yang tepat dan relevan menjadi sangat jelas, karena hal tersebut memastikan setiap tahapan penelitian diarahkan secara efektif menuju pencapaian tujuan. Oleh karena itu, pendekatan ilmiah yang dikenal sebagai metode penelitian digunakan untuk menjamin bahwa proses penelitian berjalan dengan baik dan menghasilkan temuan yang dapat dipercaya. Menurut Sugiyono (2018:2), metode penelitian didefinisikan sebagai pendekatan ilmiah untuk memperoleh data dengan tujuan dan kegunaan tertentu, yang mencakup ciri-ciri keilmuan, yakni bersifat rasional, empiris, dan sistematis (Sugiyono, 2018).

RESULT AND DISCUSSION

3.1 BSSN – KISA

The collaboration between Indonesia's National Cyber and Crypto Agency (BSSN) and the Korea Internet & Security Agency (KISA) primarily focuses on developing human resource (HR) capacity in the field of cybersecurity. The aim of this partnership is to equip Indonesian professionals with sufficient knowledge, skills, and technical capabilities to face increasingly complex and dynamic cyber threats. Through a series of training programs, workshops, and technology transfers, both institutions strive to strengthen the national cyber defense system, enabling Indonesia to effectively safeguard critical information and data. This protection directly impacts the digital rights of citizens, including privacy, personal data security, and public trust in government digital services. The cooperation encompasses various mutually reinforcing aspects, ranging from the exchange of knowledge and expertise in risk management and cyber incident handling to research and development of digital security technologies. Moreover, the collaboration emphasizes the implementation of digital signatures and the protection of vital information infrastructure, which serve as the foundation of national security in the digital era. By providing mechanisms for experience sharing and best practices, Indonesian HR is expected to adopt international standards in cyber threat mitigation and the implementation of effective security policies (Waranggani, 2022).

The training programs conducted at the Cyber and Crypto Polytechnic (Poltek SSN) in Bogor are designed comprehensively to enhance participants' competencies both technically and strategically. These trainings include cyber attack simulations, risk analysis, incident management, and the development of innovative solutions to address the evolving challenges of cybersecurity. Additionally, the collaboration highlights the importance of cross-sector cooperation among the government, industry, and academia to create a robust and sustainable cybersecurity ecosystem. Furthermore, the BSSN-KISA partnership supports the strengthening of national capacity within the framework of bilateral relations between Indonesia and South Korea, particularly under the Special Strategic Partnership. Cybersecurity is one of the key focus areas in the 2021–2025 Action Plan for the implementation of this partnership. Therefore, this collaboration not only contributes to enhancing HR technical capabilities but also reinforces digital diplomacy and international cooperation in the field of cybersecurity. In other words, the partnership underlines that human and technological capacity development is a crucial element in building national digital resilience and comprehensively protecting the digital rights of Indonesian citizens (Hardianti, 2023).

3.2 The implementation of the UU PDP

The Law Number 27 of 2022 on Personal Data Protection (PDP Law) represents a significant milestone in Indonesia's efforts to safeguard its citizens' personal data in an increasingly advanced digital era. With the rapid development of information technology, the protection of personal data has become a crucial issue to ensure the privacy rights of individuals as well as the security of information in cyberspace (jdih, 2024).

The PDP Law aims to provide individuals with greater control over their personal data and to enhance transparency in its management. The law regulates the rights of data subjects, such as the right to access, correct, and delete personal data, and establishes obligations for data controllers and processors to protect such data from unauthorized access or misuse. Accordingly, the PDP Law is expected to strengthen the protection of digital rights for Indonesian citizens. The law covers various aspects, including the principles of personal data protection, types of personal data, the rights of data subjects, personal data processing, obligations of data controllers and processors, personal data transfer, administrative sanctions, institutional arrangements, international cooperation, public participation, dispute resolution, restrictions on the use of personal data, and criminal provisions related to personal data protection (DP, 2022).

The UU PDP grants the following rights to personal data subjects:

- The right to obtain information regarding the clarity of identity, the legal basis, the purpose of the request, and the use of personal data.
- The right to complete, update, and/or correct errors and/or inaccuracies in personal data.
- The right to access and obtain a copy of personal data.
- The right to terminate processing, delete, and/or destroy personal data.
- The right to withdraw consent for personal data processing that has been previously given.
- The right to object to decisions based solely on automated processing.
- The right to postpone or limit the processing of personal data proportionally.
- The right to file claims and receive compensation for violations in the processing of personal data.
- The right to obtain and/or use personal data in a format that is readable by electronic systems.

Law Number 27 of 2022 on Personal Data Protection, which was enacted on October 17, 2022, is intended to ensure every citizen's right to personal protection and to guarantee the recognition and respect for the importance of personal data protection (siplawfirm, 2023). The implementation of the PDP Law requires active participation from the government, the private sector, and society. The government is responsible for providing the necessary infrastructure and resources, including establishing supervisory and law enforcement bodies related to personal data. Meanwhile, the private sector, particularly companies handling personal data, must comply with the provisions of the PDP Law and maintain public trust. Additionally, the public needs to be educated about their rights regarding personal data and how to protect them. Although the PDP Law has been enacted, its implementation still faces several challenges, such as low public awareness of the importance of personal data protection, limited resources for oversight, and the need for more detailed implementing regulations. However, with a shared commitment from all parties, the PDP Law is expected to be effective in safeguarding the personal data of Indonesian citizens.

Law Number 27 of 2022 on Personal Data Protection marks a significant advancement for Indonesia in safeguarding its citizens' personal data in the digital era. By establishing the rights of data subjects, the responsibilities of data controllers and processors, and sanctions for violators, the PDP Law aims to create a secure and trustworthy digital ecosystem. Effective implementation of this law requires collaboration among the government, the private sector, and society to ensure that personal data is properly protected and individual rights are respected.

3.3 Forms and Implementation of the Cooperation

The signing of a Memorandum of Understanding (MoU) between Indonesia's National Cyber and Crypto Agency (BSSN) and the Korea Internet & Security Agency (KISA) took place on October 17, 2022, as a demonstration of both countries' commitment to strengthening national cybersecurity capacity. This cooperation is designed to cover various strategic and operational areas that complement each other, aiming not only to enhance technical capabilities but also to reinforce policy frameworks, regulations, and cybersecurity infrastructure in Indonesia.

1. Human Resource Development

   A primary focus of this cooperation is the development of skilled professionals in the field of cybersecurity. To achieve this goal, BSSN and KISA organize joint training and educational programs across multiple levels, ranging from basic to advanced professional training. One significant initiative is the establishment of the Cyber Security Vocational

Center (CSVC) at the Cyber and Crypto Polytechnic (Poltek SSN) in Bogor. This program is designed to equip participants with practical skills and strategic understanding of cybersecurity, including cyberattack simulations, risk analysis, incident management, and the development of innovative solutions. Through these trainings, Indonesia aims to produce professionals capable of addressing increasingly complex cyber challenges, while also supporting the creation of a robust and sustainable national cybersecurity ecosystem (Hardianti, 2023).

2. Knowledge and Technology Exchange

   In addition to HR development, this cooperation emphasizes the importance of exchanging knowledge and technology between the two agencies. BSSN and KISA actively share experiences, best practices, and international standards in risk management, incident mitigation, and data security. Furthermore, the collaboration includes research and development in cybersecurity technologies, the implementation of digital signatures, and the protection of vital information infrastructure that forms the backbone of national security. Through technology transfer, Indonesia can adopt advanced security methods and systems proven effective in South Korea while adapting them to local needs and contexts (palupi, 2022).

3. Policy and Regulatory Strengthening

   The BSSN-KISA cooperation also includes support in formulating stronger cybersecurity policies and regulatory frameworks. KISA provides guidance on international standards, best practices, and effective implementation strategies, which BSSN then adapts to Indonesia's legal and operational context. This not only aids in developing relevant national regulations but also facilitates Indonesia's integration into the global cybersecurity ecosystem.

4. Impact and Benefits of Implementation

   The implementation of this cooperation has a direct impact on enhancing national capacity. With training programs and technology transfer in place, HR competencies improve, risk management becomes more structured, and response to cyber incidents is faster and more accurate. Additionally, the protection of personal data, privacy, and critical infrastructure is strengthened, thereby increasing public trust in government digital services.

Overall, the forms and implementation of the BSSN-KISA cooperation are not only technical but also strategic. By combining HR development, technology exchange, and policy strengthening, this cooperation builds a solid foundation for Indonesia's national cyber resilience and enhances the country's capacity to face cybersecurity challenges at both regional and global levels.

CONCLUSION

This study highlights the strategic role of the collaboration between Indonesia's National Cyber and Crypto Agency (BSSN) and the Korea Internet & Security Agency (KISA) in protecting Indonesian citizens' digital rights. The partnership focuses on developing cybersecurity human resources, technology transfer, knowledge exchange, and strengthening relevant policies and regulations. The collaboration enhances technical capabilities, reinforces national cybersecurity systems, and safeguards privacy, personal data, and digital rights. Initiatives such as training at Poltek SSN and the establishment of the Cyber Security Vocational Center (CSVC) exemplify its implementation. Moreover, the partnership supports digital diplomacy and integration into the global cybersecurity ecosystem, ensuring recognition of digital rights both nationally and internationally. Despite challenges like regulatory differences and resource limitations, the collaboration is crucial for building national digital resilience and securing the digital rights of Indonesian citizens.

REFERENCES

antara. (2022). *BSSN Menjalin Kerjasama dengan Korea Selatan Tingkatkan Keamanan Ruang Siber.* jogja.antaranews.com.

Ayu, M. G. (2022). *BSSN: Keamanan Siber Penting dalam Menjadmin Transformasi Digital.* digitalcitizenship.id.

Center, I. N. (2022). *BSSN and Microsoft Partner for Threat Intelligence Sharing to Combat Rising Cybercrime in Indonesia through Cyber Threat Intelligence Program.* news.microsoft.com.

csirt. (2022). *In an effort to strengthen national cybersecurity capabilities, BSSN has established a strategic partnership with the Korea Internet & Security Agency (KISA) of South Korea. The cooperation agreement between BSSN and KISA was officially signed on July 21,.* Makassar: csirt.makassarkota.go.id.

DP. (2022). *Perlindungan Data Pribadi.* Jakarta: peraturan.bpk.go.id.

Dugis, V. (2016). *Teori Hubungn Internasional.* Surabaya: Cakra Studi Global Strategis (CSGS).

Hardianti, C. (2023). *Kerjasama Indonesia Korea Selatan dalam mempertahankan Keamanan Siber Nasional di Indonesia.* Makassar: Repositori UIN Alauddin.

Humaira, N. (2023). *5 Definisi Hubungan Internasional Menurut Para Ahli.* Detikedu.

jdih. (2024). *Undang Undang no 27 tahun 2022 Tentang Perlindungan Data Pribadi.* Semarang: jdih.semarangkota.co.id.

News, L. (2023). *Telusuri Lebih Jauh Bidang Hubungan Internasional.* Jakarta: LSPR.

palupi, Y. P. (2022). *Kerjasama dengan KISA, BSSN Tingkatkan Keamanan Ruang Siber.* koranbernas.id.

siplawfirm. (2023). *Jenis dan Hak Subjek Data Pribadi Dalam UU PDP.* Jakarta: siplawfirm.id.

Sugiyono, P. D. (2018). *Metode Penelitian Kombinasi (Mixed Methods).* Bandung: Alfabeta.

UNDP. (1994). *Human Development Report 1994.* hdr.undp.org.

Waranggani, A. S. (2022). *Kolaborasi BSSN dan Korea Selatan untuk Perkuat Cyber Security.* csirt.or.id.