

Strategy for Enhancing Indonesia's Cybersecurity Policy

Rengga Vernanda¹, Afifah Rahmawati

Lembaga Administrasi Negara¹

Abstract

The development of information technology has changed the world landscape with the existence of an area called cyberspace. The rapid development of cyberspace, which is integrated with aspects of human life and has far-reaching effects on the links of life, has made cyber security one of the most important issues in the world. The number of cybercrime cases that occur requires the acceleration of cybersecurity reform in Indonesia. This study aims to outline the challenges and problems of cybersecurity in Indonesia and provide several alternative policies that can be taken by the Indonesian government to strengthen cybersecurity in Indonesia. This study uses a literature review approach by utilizing data and documents related to cybersecurity in Indonesia. The results of the study show that the challenges faced by the Indonesian government today are, firstly, cybersecurity policies in Indonesia are still overlapping, secondly, the need for institutional improvement and authority over data protection and cybercrime, and finally, the human behavior factor in the emergence of cybersecurity. Based on some of these problems, it is necessary to submit policy recommendations, namely, first, the need for the Government of Indonesia to improve the quality and capability of the Indonesian people about the importance of cybersecurity, second, the Government of Indonesia needs to immediately ratify the draft law on cybersecurity, third, the need to strengthen the duties, functions and authority of the State Cyber and Crypto Agency (BSSN), and the last recommendation is to increase the cooperation and involvement of the Indonesian government with cyber security institutions at the international level.

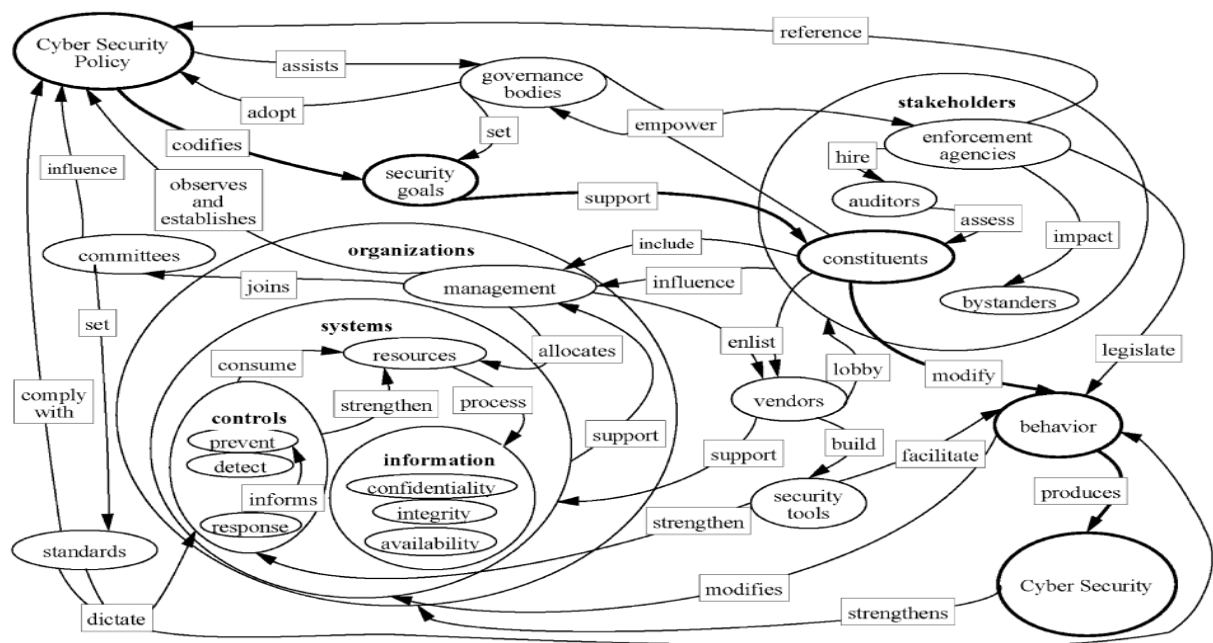
Keywords: *cyberspace, cybersecurity, policy, BSSN*

1. Introduction

The digital revolution, sometimes referred to as cyber-civilization, has completely changed how people interact, communicate, search for information, do business, and otherwise function and transform the processes of human life. The speed and scale of change have made the Internet both an indispensable channel for information exchange and a part of modern life. The developments in information and communication technology are utilized by individuals and organizations across a multitude of sectors including banking, healthcare, government, education, human resource management, smart city initiatives, network systems, and various other domains [1]. While these technological advancements have facilitated the execution of tasks and activities, they also present significant security challenges that require attention from all parties involved, ranging from individual users to governmental entities [2].

The development of cyber civilization is going on at a fast pace and getting integrated with almost all aspects of human lives, having a great impact on the inter-related dimensions of life, which makes cybersecurity one of the most important issues in the world [3]. It is defined as cybersecurity that refers to an attempt to protect the confidentiality, integrity, and availability of computing resources owned by an organization so that they can securely connect with a network of other related entities [4]. According to [5], the cyberspace will be a complicated domain for any organization if there is no ability to control access to network systems and proprietary information. If cybersecurity can be well implemented, cyberspace is a reliable, robust, and also a trustworthy digital platform. Through reliable cybersecurity, organizations will have defense mechanisms, intrusion detection mechanisms, and encryption mechanisms from threats that will harm the organization [6].

Bayuk [5] defined cybersecurity as the capability to control access to networked systems and to the information hosted in those networked systems. If such controls can effectively be executed, then the cyberspace becomes a dependable, resilient, and trustworthy digital infrastructure. On the other hand, if cybersecurity controls are not well designed and deployed, the cyberspace will become a wild world in the digital civilization.



In this figure, the government was acting as the regulator in the application of the cybersecurity policy: it provides the laws, standards, and rules that would affect the way data and information are distributed, information protected, or even behavioral habits of the stakeholders. Additionally, there will be security for both internal and external data provided by the organisational circle that may use the policies set by the government in defining the minimum standards an organisation must meet in controlling, preventing responding to, and mitigating. Also, it's ensured at the vendor node that the cybersecurity policy must facilitate the enabling of vendors to support effectively creating a cybersecurity climate; hence, a tool to support and enable the implementation of such policies in order to support cybersecurity with the provided products and services. Whereas the stakeholders or user groups have the possibility of giving inputs, carrying out evaluations for further improvements in the established cybersecurity policies.

The new millennium challenges the Indonesian government to address cybersecurity as one of its major problems. During the end of 2023, BSSN [8] published a comprehensive report related to the cybersecurity landscape in Indonesia. It is documented that 403,990,813 identified traffic anomalies were observed. These unusual traffic activities can lead to reduced device and network performance, theft of sensitive data, damaged reputation, and decreased confidence in an organization. In fact, even from the BSSN team's search of the darknet, there were 1,674,175 data exposures affecting 429 agencies. Darknet exposure indicates a case where data or account credential information related to a specific agency or organization is available on the darknet, including data trading platforms, forums for hacker discussions, or instant messaging services, thereby allowing chances for unauthorized individuals to exploit this information. Further analysis of the exposure data, in fact, denotes that the highest total exposure to the government sector at 39.78%, is followed by the financial sector at 9.86%, ICT sector at 9.63%, transportation sector at 3.40%, ESDM sector at 1.75%, health sector at 0.23%, food sector at 0.2%, and the defense sector at 0.12%, while other sectors have 35.04% thereof.

Cyber attacks in the form of data leakage are an important concern to the government of Indonesia. In February 2021, a teenager, only 16 years old, hacked the database of Attorney General's Office of the Republic of Indonesia for leisure. The data leak has exposed 3,086,224 records and was sold for about Rp 400,000. In May 2021, 272 million BPJS records are also leaked and have been publicly offered by cyber hackers on the internet. The leaked data contains participants' personal data and their family from BPJS Kesehatan and the salary information of the participants. It is suspected that this data breach was assisted by external parties or vendors, in that sufficient audits and checks were not done. Another cyber attack occurred in September 2022 where at least 1.3 billion SIM card records were leaked. Information such as the identity numbers and contact details transacted commercially on the internet for a sum of US\$50,000. The most recent incident of cybercrime in the form of data theft is the leakage of information at the Temporary National Data Center, which crippled many public services, such as the NPWP registration service online, the paralyzing of the immigration system digitally, and state losses of Rp 6.3 trillion.

Due to these incidents, cybersecurity has now become integral to the innovation of new technology, services, and even governmental policies. In fighting cybercrime, there needs to be a detailed and more secure strategy worked out; therefore, fighting cybercrime cannot be done through technical means only. Governments have to be capable of developing such a policy framework that reinforces cybersecurity to the extent that it is able to investigate and prosecute cybercrime. Whereas, to enhance security, reduce security risks, strengthen cybersecurity, build up cybersecurity policies, educate and create awareness for increasing the importance of cybersecurity and how to avoid attempts of data theft, many precautionary measures have really been considered and addressed. However, within this very phenomenon, crimes within cyberspace are on their way to growth.

2. Method

This study uses a literature review approach as the main data collection and analysis activity. Literature study, or literature review, is information gathering through review, collection, and analysis of various literatures relevant to the research topic. The research method for this study was chosen based on its ability to provide more in-depth insight by delving into the existing data, concepts, and policies related to the field of cybersecurity. The literature review was based on sources from books or reports encompassing data on cybersecurity in Indonesia. Further analysis was also drawn from data emanating from government policies related to cybersecurity. Other data were adapted from articles in journals whose findings had, in one way or another, some relevance to cybersecurity in Indonesia. The contents of the data gathered will then be analyzed. The aim of the content analysis is to identify data, problems, challenges, and ideas emerging from the various literature sources read.

3. Results and Discussion

The government of Indonesia issued various policies in order to face the threat and potential of cybercrime. The efforts made still have some shortcomings, especially in the implementation part. National Cyber Security Index (NCSI) data in 2023. NCSI or National Cyber Security Index, Indonesia's cyber security is ranked 49th out of 176 countries. In this ranking, Indonesia was ranked fifth in Southeast Asia. Based on the ranking, Indonesia got a score of 63.64. This number is above Malaysia (79,22), which has the best cyber security in Southeast Asia, followed by Singapore (71,43), Thailand (64,94), and the Philippines (63,64). The NCSI index might be one of the references for a country's implementation of cybersecurity. The NCSI represents an internationally recognized index in measuring the readiness to deter cyber attacks and handling the cyber incident in the country. Measurement using NCSI concentrates on measurable aspects of cybersecurity conducted by the government of a country. The aspects are

1. Cybersecurity policy development
2. Cyber threat analysis and intelligence
3. Education and training
4. Contribution to global cyber security
5. Protecting digital services
6. Protecting critical services
7. Electronic identification and trust in services
8. Protecting personal data
9. Cyber incident response
10. Cyber Crisis Management
11. Combating cybercrime
12. Military cyber operations













40.		Norway	67.53	<div><div></div></div>	80.19	<div><div></div></div>	-12.66
41.		Cyprus	66.23	<div><div></div></div>	68.83	<div><div></div></div>	-2.60
42.		Australia	66.23	<div><div></div></div>	77.61	<div><div></div></div>	-11.38
43.		Luxembourg	66.23	<div><div></div></div>	78.40	<div><div></div></div>	-12.17
44.		Georgia	64.94	<div><div></div></div>	53.50	<div><div></div></div>	11.44
45.		Thailand	64.94	<div><div></div></div>	56.63	<div><div></div></div>	8.31
46.		United States	64.94	<div><div></div></div>	81.05	<div><div></div></div>	-16.11
47.		Paraguay	63.64	<div><div></div></div>	42.58	<div><div></div></div>	21.06
48.		Philippines	63.64	<div><div></div></div>	45.99	<div><div></div></div>	17.65
49.		Indonesia	63.64	<div><div></div></div>	47.41	<div><div></div></div>	16.23
50.		Azerbaijan	63.64	<div><div></div></div>	54.78	<div><div></div></div>	8.86
51.		Argentina	63.64	<div><div></div></div>	60.43	<div><div></div></div>	3.21

Figure 4: National Cyber Security Index

The report released by NCSI reports that Indonesia is in the first category, namely, the development of cybersecurity policy; Indonesia does not get a good score of 43% because there is only one indicator that has been filled in, namely the existence of an agency authorized to address the issue of cybersecurity, in this case, the BSSN. In the subcategory, there is no national committee formed by the government to coordinate cybersecurity. Moreover, Indonesian government is also considered not to have any cybersecurity plan or strategy at the national level, so that Indonesian government only scored 43% in this category.

While in the second category, cyber threat analysis and intelligence, Indonesian government scored 40%. Based on inability to fulfill the greater part of the existence of government institutions playing an important role at the national level in analyzing the cyber threat situation. For the third aspect, education, and professional development, Indonesia scored 67% since there was no identified educational curriculum that avails cybersecurity competency. While contributing to global cybersecurity, Indonesia got

a poor score of 17% because the Indonesian government has never contributed to international agreements regarding cybersecurity. Besides that, Indonesia has never participated either in organizing or funding the capacity building activities of other countries in the field of cybersecurity.

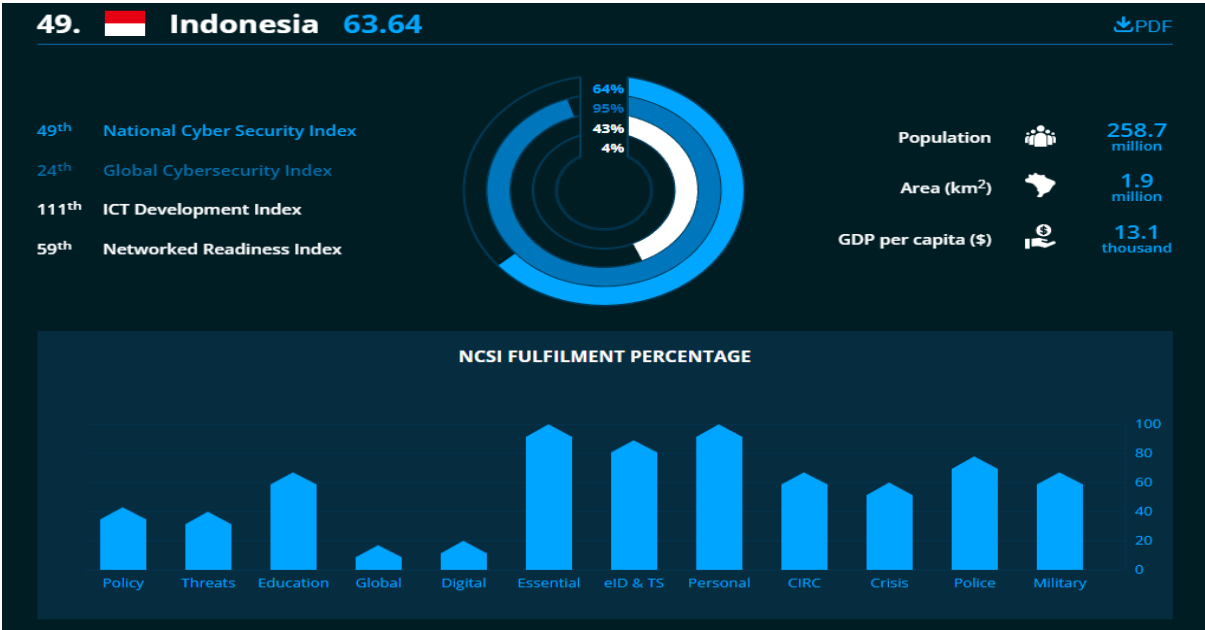


Figure 5. Assessment Aspects of Indonesia's National Cybersecurity Index

In addition, Indonesia again received a poor score of 20% in categories related to the protection of digital services. In this category, Indonesia only meets the protection policy for the implementation of electronic systems and transactions contained in PP Number 71 of 2019 on the Implementation of Electronic Systems and Transactions. Meanwhile, according to NCSI, digital services in Indonesia fall into a category considered not to meet minimum requirements for digital public services implemented by the Indonesian government. Moreover, this is also in consideration that the Indonesian government does not have a unit tasked with providing an assessment of the cybersecurity of digital services in Indonesia. It is of important service protection, while the Indonesian government has a maximum score of 100%, because it can meet each criterion such as the existence of regulatory policies, the existence of units that can give security assessments and controls, and the existence of publications by each service provider agency.

In the category of electronic identification and trust in services, the Indonesian government obtained a good score, which was 89%. Its shortcoming was that the cryptographic ecosystem was not regulated. Digital identity: It was taken into consideration that in respect of the digital signature and based on the institutions that guarantee its operation, these services were good enough. The Indonesian government scored well in personal data protection. This is owing to the existence of Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection. The next category is Response to Cyber Incident, where it has not been decided by the Indonesian government as to who the single point of contact for cybersecurity coordination is. In this category, already, the Government of Indonesia has a certain unit responsible for detecting and serving responses against cyber threats. The next category is Cyber crisis management; the Government of Indonesia got a score of 60% because NCSI believes that the Government of Indonesia does not yet have a major plan to deal with major cyber incidents. Besides, there is no procedure for the use of volunteers as required by law. The next category is fighting cybercrime, where the Indonesian government scored 78%. NCSI considers the Indonesian government to be quite

good at fighting cybercrimes that happen. The last category is about cyber military operations; it can be said that the Indonesian government scored quite well with 67%. That is because Indonesia already has a special unit in the TNI, tasked to carry out the cyber operation—that is, Satsiber TNI. The Indonesian government is, however, still seen to be lacking in this category, especially in the way the published cyber operation exercises are not enough, particularly within the last three years.

Besides the data given by the NCSI, the Indonesian cybersecurity policy remains fragmented. It is seen from the many cyber securities that have been issued by the Indonesian government, for example: Ministry of Defense Regulation No. 82/2014 concerning Guidelines for Cyber Defence and Presidential Regulation No. 47/2003 on National Cybersecurity Strategy and Cyber Crisis Management. In the context of cyber defense policy in the Ministry of Defense Regulation, it was only applied within the function of military cyber defense, which was developed and implemented through the cooperation between the Ministry of Defense and the Indonesian National Army through the TNI Cyber Unit. On the contrary, according to Presidential Regulation Number 47/2023, BSSN is in charge of handling cyber security. Furthermore, the establishment of a directorate related to cybercrime in POLRI is also supported by Law No. 19/2016 on ITE. Such ambiguity then turns into an anomaly in the practice of national cyber security, particularly in terms of what policy should be enacted as a common guide in relation to cyber security.

The second problem is related to institutionalization and authority regarding data protection and cybercrime. One of the significant cybersecurity cases that occurred in Indonesia involves hacking 1.3 billion pieces of SIM card data. This case involves the Ministry of Communication and Information, the Directorate General of Population and Civil Registration within the Ministry of Home Affairs, and cellular service providers as those having authority to take responsibility for the breach in data. Indeed, this cannot be separated from the ambiguity of the institutions that have authority over data security. This ambiguous institution becomes another highlight for the NCSI, especially within the cybersecurity policy development category, in that a national committee formed by the government is needed in order to coordinate cybersecurity.

Another aspect on which Indonesian government needs to take into consideration is human behavioral factors in implementing cybersecurity reforms. Based on data from Verizon's cybercrime report, as reported by [10], it shows that 85 percent of all breaches hence include human behavioral elements. It is presented as evidence in this data, the forensic result of the cause of cyber attacks in some incidents that occurred in Indonesia. For example, cases include the theft of 3.086.224 Kejaksaan Agung RI data, which was carried out by a 16-year-old child with the motive of playing a prank. Then there is the hacking of the PDN temporary data as a result of negligence in the use of password. The Minister of Communication and Information Technology who is going to sign the regulation of Ministry of Communication and Information Technology, concerning the obligation of ministries/institutions for data backup, does not understand or even know the importance of data security in terms of human resources. Article 40, paragraph 4 of Law Number 19/2016 indeed obliges ministries and agencies to make electronic documents and records, and connect them to a certain data center for the purpose of data security. According to [5], from the perspective of cybersecurity, human behavior should become an integral part of building a more comprehensive cybersecurity system. The policymakers will be taught how human behavior can be used in the building of new tools that can reduce cybersecurity threats.

Looking at the challenges and problems of cybersecurity in Indonesia, it is necessary that recommendations should be submitted to the government for improvement and acceleration in this regard. From an integrated perspective in cybersecurity, people should be aware of the risks they face on the Internet and know how to protect themselves. The business sector must take measures that are necessary concerning security; only then can data protection be ensured. Meanwhile, it is the

government's job to ensure that people and businesses are doing the right thing by making the right laws. Just like in physical security, if all parties can cooperate, we can minimize or even mitigate the impact of cyber incidents.

First recommendation, The need to improve the quality and capability of the Indonesian people by the Government of Indonesia regarding the importance of cybersecurity. It can be enhanced in quality and capability through socialization, which is coordinated and continuous, both in central and regional agencies, on the importance of cybersecurity and the importance of protecting vital information infrastructure. This socialization is expected to avoid or minimize disruption to cybersecurity because of the element of human negligence. Socialization can be done by utilizing public space in the community through social media, collaboration with influencers, establishing a cybersecurity awareness campaign movement, and taking advantage of volunteers to spread the cybersecurity movement.

Second recommendation immediately, the Indonesian government needs to enact the Cybersecurity Law, which can be the basis for the government agencies in mitigating cybersecurity, especially to prepare the quality of infrastructure and prepare national vital data, and also to know the level of readiness and security of national digital security. This cybersecurity law will enable the Indonesian government to coordinate and stipulate the main agencies responsible for mitigating, identifying, implementing, and evaluating cybersecurity in Indonesia. Under this law, those agencies which have cybersecurity units, such as TNI, POLRI, and BSSN, may coordinate and cooperate in maintaining Indonesia's cyber civilization. The government needs to convince the legislature about the importance of cybersecurity in Indonesia and encourage it to be a priority policy in national legislation in order to ratify this policy immediately. Besides accelerating the ratification of the Cybersecurity Law, the Indonesian government is also obliged to update the Cybersecurity Operational Law every two years. It is something that cannot be parted or set aside from the rapid development of cyberspace. Therefore, it needs to be accompanied by the renewal of cybersecurity policies such as the development that needs to be covered, which ranges from cybercrime to cyber military and cyber intelligence.

Next recommendation is there has to be strengthening duties, functions, and authority of State Cyber and Crypto Agency (BSSN). The draft law on cybersecurity must be able to strengthen the duties, functions, roles, and authorities of the BSSN. With the prevailing conditions, the BSSN is only given the authority to coordinate, not to be responsible for, or to regulate the data security procedures in other agencies. A soon-to-be-promulgated Cyber Security Law will set BSSN as the only authority to determine the policies and instruments of national cyber security, which today are scattered amongst institutions such as TNI, Polri, and also those within the ranks of cyber security teams in each government agency. Strengthening the BSSN's role by taking authority from other institutions will most likely create sectoral conflicts; therefore, the BSSN must be able to adopt a multi-stakeholder approach and cooperate in creating a data security ecosystem for each activity in cyberspace.

Last recommendation is enhance the Indonesian Government's cooperation and engagement in cybersecurity institutions at the international level. Among the areas the NCSI pointed out was the very minimum contributions of Indonesia towards global cybersecurity. In the contemporary world of globalisation and interdependence, problems and prospects of a country are not exclusively local, but also regional and international. Hence, the sole prerequisite for an inclusive and sustainable consensus demands the coming together of stakeholders at the varied local, regional, national, private sector, and state levels. This would, therefore, be able to establish a cyber defense that is resilient, adaptive, and responsive to various cyber threats that might evolve. The government of Indonesia can encourage the establishment of cybersecurity cooperation among countries as one of the ASEAN member countries. In other words, all this cooperation will by no means be easy, considering that each country has something

different in their perspectives and motivations; therefore, a strategy which can harmonize the motivations and create mutually beneficial cooperation in the field of cyber security will be needed. It can be achieved through information exchange, cooperation in organizing cybersecurity training and skills between countries, and role exchange between industry and government.

4. Conclusion

Cybersecurity policy is a strategic step that must be taken by the government to deal with the development of cyberspace and cyber threats. In the results of data analysis, three challenges are presented that need to be addressed by the government, namely, *first*, cybersecurity policies in Indonesia are still overlapping, *second*, there is no clear institutional and authority on data protection and cybercrime, and *third*, human behavior factors in the implementation of cybersecurity reforms. In order to overcome these challenges, strategic steps are needed, which include, *first*, the need for the Indonesian government to improve the quality and capability of the Indonesian people about the importance of cybersecurity; *second*, the Indonesian government needs to immediately pass the Cybersecurity Law; *third*, the need to strengthen the duties, functions, and authority of the State Cyber and Crypto Agency (BSSN); and *finally*, the Indonesian government needs to increase cooperation and involvement with cybersecurity institutions at the international level.

5. References

- [1] Admass, Wasyihun & Yayeh, Yirga & Diro, Abebe. (2023). Cyber Security: State of the Art, Challenges and Future Directions. *Cyber Security and Applications*. 2. 100031. 10.1016/j.csa.2023.100031.
- [2] M.Z. Gunduz, R. Das, Cyber-security on smart grid: threats and potential solutions, *Comput. Netw.* 169 (2020) 107094, doi:10.1016/j.comnet.2019.107094.
- [3] G.W. Peters, E. Panayi, Understanding modern banking ledgers through blockchain technologies: future of transaction processing and smart contracts on the internet of money, *SSRN Electron. J.* (2015) 1–33, doi:10.2139/ssrn.2692487.
- [4] F. Ullah, H. Naeem, S. Jabbar, S. Khalid, M.A. Latif, F. Al-Turjman, L. Mostarda, Cyber security threats detection in internet of things using deep learning approach, *IEEE Access* 7 (2019) 124379–124389, doi:10.1109/ACCESS.2019.2937347.
- [5] Bayuk, J. L. (2012). *Cybersecurity policy guidebook: An introduction*. John Wiley & Sons.
- [6] G.D. Rodosek, M. Golling, Cyber security: challenges and application areas, *Lect. Note. Logist.* (2013) 179–197, doi:10.1007/978-3-642-32021-7_11.
- [7] Badan Siber dan Sandi Negara, *Lanskap Keamanan Siber Indonesia 2023*, Jakarta: BSSN: Januari 2024. Available from: <https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf>
- [8] Budi E., Wira D., dan Infantono A. Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia, Akademi Angkatan Udara | Yogyakarta, 24-25 November 2021* Volume 3, Tahun 2021, hlm. 223-234 DOI:10.54706/senastindo.v3.2021.141
- [9] Gallaher, M. P., A. N. Link, et al. (2008). *Cyber Security, Economic Strategies and Public Policy Alternatives*. Cheltenham, UK: Edward Elgar
- [10] Yeo LH, Banfield J. Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis. *Perspect Health Inf Manag.* 2022 Mar 15;19(Spring):1i. PMID: 35692854; PMCID: PMC9123525