National Defense Model Based On Data Sovereignty: Strategy To Overcome Threats In Digital Era

Januar Arief Martharaharja[1)],Romie Oktovianus Bura[2)]
[1,2.] *Faculty of Defense Technology, Indonesia Defense University, IPSC Area, Bogor and 16810, Indonesia*
Email: januar.martharaharja@idu.ac.id

Submit: 14th March 2021, Revised: 08 th March 2021 , Accepted: 29 th March 2021

Abstract.*Threats to national defense and security always develop along with technological advancements. The threat does not only come from the real world which involves physical attacks, but can also come from cyberspace in the form of attacks on the security of state data. The purpose of this research is to develop a national defense model based on the concept of data sovereignty to overcome various threats that come from the digital world. The type of this research is descriptive qualitative with research data in the form of secondary data collected using literature studies and analyzed using qualitative techniques. The model of national defense based on data sovereignty illustrates the components needed to shape national defense. These components consist of policy, institutional, law enforcement, and various other components that contribute to building data sovereignty.*

Keywords: Data Sovereignty, National Defense and Security, Digital Era, Cyber Threats

I. INTRODUCTION

Indonesia is a sovereign country and always strives to remain sovereign through the development of its defense and security. According to Presidential Regulation No. 5/2010 concerning the National Medium-Term Development Plan (RPJMN) 2010-2014, the Defense and Security sector covers all tasks and functions carried out by eight state institutions consisting of the TNI, Polri, National Intelligence Agency (BIN), The State Code Institute (Lemsaneg), the National Narcotics Agency (BNN), the National Defense Agency (Lemhanas), the National Defense Council (DKN), and the Maritime Security Coordination Agency (Bakorkamla). Those eight institutions work together in building defense and security with the aim of upholding the country's sovereignty, maintaining the integrity of the Unitary Republic of Indonesia, safeguarding the safety of all nations from military and non-military threats, increasing the sense of security and security of activities, staying orderly and upholding the law in the community, and ensuring security and comfort conditions as a guarantee of the conducive investment climate (Jazuli, 2016).

Along with the development of technology, the need for the development of efforts to maintain defense and security also continues to increase due to the emergence of new model threats that utilize advanced technology, or what is known as cyber threats. Therefore, the government through the Republic of Indonesia Presidential Regulation No. 53/2017 concerning the State Siber and Code Agency forms a non-ministerial institution called the State Siber and Code Agency (BSSN). This institution is a development of the State Code Institute (Lemsaneg) with a special task to implement cyber security effectively and efficiently by utilizing, developing, and consolidating all elements related to cyber security.

The formation of BSSN with its specific task represents the government's seriousness in facing threats from the digital realm towards state sovereignty. This government decision is based on various consideration by referring to evidence regarding the impact and massive damage from cyber attacks, such as findings from McAfee, a well known computer antivirus company, which states that the global loss from cyber attacks in 2017 has reached around IDR 8.160 trillion or US $ 600 billion (Franedya, 2018). This number is expected to continue to increase rapidly given the increasing number of internet users. Every internet user can be a prospective party who launches a cyber attack or vice versa, becomes a victim of the attack. The potential increase in the number of cyber attacks and the resulting damage can be seen in McAfee's findings which show that up to the first quarter of 2019 there were almost one billion new Malicious Software (Malware) used in cyber attacks worldwide (McAfee.com, 2019).

Malware is a computer program that was developed with the aim of entering a computer

system clandestinely and damaging it. Through the existence of the internet, malware has unlimited target range, as long as there is interaction between computer systems that are connected to the internet and exposed to malware. This destructive program can enter the computer system via email, inflitrates through a program or application downloaded from the internet, or through files that have been exposed to malware. The impact and damage caused by the presence of malware in a computer system is diverse, ranging from the loss of the authority of the computer owner to use his computer, the damage to programs installed in the computer, the damage to the whole computer system, to the theft of important data contained in the computer infected with malware(Tedyyana & Supria, 2018).

Besides in the form of malware, there are several other types of cyber attacks, namely hacking, cracking, cyber sabotage, and spyware. Hacking is a cyber attack that is launched by entering the victim's computer system to take the authority of its operations and then use it in accordance with the wishes of those who carry out the hacking (hacker). Cracking is done by peeking confidential data from credit card holders, then using these data to meet the interests of the perpetrators of cracking. Cyber sabotage is done by making interference, destruction of data and computer network systems that are connected to the internet. Spyware is a cyber attack carried out by secretly recording various activities of online users, and then selling the recorded data to interested parties for advertising purposes or to spread viruses (Rahmawati, 2017).

According to McAfee's research results, cyber attacks were carried out with specific targets consisting of nine target categories, namely health organizations, the public sector, educational institutions, individuals, financial institutions, entertainment businesses, media, retail, and the technology industry. The public sector is the main target of cyber attacks among other targets, followed by individual targets as the second target, then health organizations, financial institutions, educational institutions, media, entertainment businesses, retail, and finally the technology industry (McAfee.com, 2019).

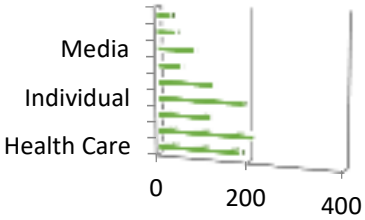


Figure 1. Target of Cyber Attack in 2018-2019
Source: McAfee.com (2019)

The source of the cyber attacks mostly came from the United States by 75%, then China and Germany each by 4%, then Brazil and Italy each by 3%, and the rest from other countries by 11%(McAfee.com, 2019).

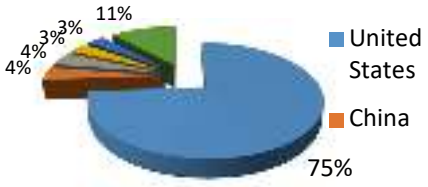


Figure 2. Source of Cyber Attack
Source: McAfee.com (2019)

As for the scope of Indonesia, BSSN managed to find that during 2018, the number of cyber attacks that attacked Indonesia was 12.895.554 attacks, with a total number of malware attacks of 513.863 attacks. The countries that were the biggest sources of cyber attacks on Indonesia were Russia with a total of 2.597.256 attacks; then China 1.871.363 attacks; United States 1.428.440 attacks; Singapore as many as 1.030.769 attacks; Netherlands 964.482 attacks; France as many as 775.257 attacks; from within the country (Indonesia) as many as 713.878 attacks; India 674.689 attacks; Canada 493.897; and from Germany as many as 211.310 attacks (BSSN, 2018).

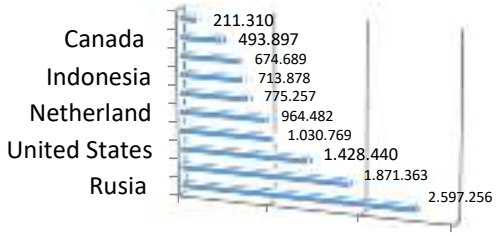


Figure 3. Country of Origin of the Cyber Attack on Indonesia in 2018
Source: Annual report of BSSN (2018)

The data above shows that cyber attacks will continue to be one of the biggest threats that will be faced by Indonesia in the future. Even the potential loss of the country in 2018 due to cyber attacks is

estimated to reach US $ 34.2 billion or around IDR478.8 trillion (Gewati, 2019). Therefore, extra hard and sustainable efforts are needed to increase national defense, especially in the digital sphere to defend Indonesia's sovereignty from threats and cyber attacks.

According to Minister of Defense Regulation No. 82/2014 concerning Cyber Defense Guidelines, there are three types of cyber threats, namely Hardware Threats, Software Threats, and Data/Information Threats. Hardware Threats are threats that are caused by the installation of certain equipment to carry out certain activities in a system, so that the equipment is a disruption to other Network and Hardware systems, for example Jamming and Network Intrusion. Software Threats are threats caused by the entry of certain software to carry out activities such as Information Theft, Information Damage, information manipulation and so on, into a system. Data or information threats are threats that result from the dissemination of certain data or information aimed at specific interests.

The biggest cyber threat among those three types of threats is the data threat because data is the most valuable asset in the world today. The party who is able to master the data will be the main determinant of further world developments. Conversely, those who are unable to maintain and manage their data will be eliminated from competition in all fields and will even have difficulty to survive (Hummel, Braun, Augsberg, & Dabrock, 2018). Considering that Indonesia as a developing country is still lagging behind in the development of information technology, cyber threats in the category of data or information threats are becoming increasingly urgent to anticipate (Rizal & Yani, 2016).

In this regard, the instruction given by Indonesian President Joko Widodo is to realize data sovereignty, namely by protecting confidential data from all threats of cyber attacks (Prasetia, 2019). Data sovereignty is one of the main foundations of national defense, especially in dealing with various cyber threats and to create cyberspace sovereignty. This is important to be realized in order to get two important benefits of cyberspace sovereignty, namely the benefits in the form of state welfare and the benefits of national security (Cahyadi, 2016).

Based on the overall explanation above, this research was carried out with the aim to develop a national defense model based on data sovereignty that can be used to overcome cyber threats in the digital age. These objectives are further specified into a number of specific objectives, including determining the components of national defense in the digital age, which consist of policy, institutional, law enforcement, and various other components that contribute to building data sovereignty.

II. LITERATURE REVIEW

This research IS conducted with reference to previous research that has relevance to the topic of data sovereignty in relation to national defense. The first prior research was conducted by Rahmawati (2017) entitled “Risk management analysis of cyber crime threats in increasing cyber defense”. The research aims to identify risk management to be able to find out how big the probabilities and consequences arising from cyber crime. The identified risks are used as the basis for formulating a national defense strategy in facing the threat of cyber crime. The type of the research is descriptive qualitative using secondary data obtained from literature studies. Data analysis was performed using qualitative techniques. The results of the study stated that the government through the Ministry of Defense institution needs to prepare themselves in facing cyber threats. The Ministry of Defense needs to prepare reliable Human Resources in mastering technology, reliable infrastructure systems, and supported by legislation or policies in carrying out cyber warfare operations. In addition to a strong national defense, legal support is also needed that affect each other and are interconnected in dealing with the threat of cyber crime. The need for proper regulation and cooperation with all parties, both government and private sector, can become the main key in facing the increasingly complex challenges of the cyber world.

The second previous research by Arianto & Anggraini (2019) entitled “Building Indonesian national cyber defense and security in order to deal with global cyber threats through the Indonesia security incident response team on internet infrastructure(ID-SIRTII)**”.** The aim of the research is to explore the importance of ID-SIRTII in preventing global cyber threats. The results of the study found that the threat of cyberspace in Indonesia is very complex, with variations of actors, motives, and targets. This complexity can be explained through the following four aspects, namely: 1) dEparting from the study of Geometripolitika, cyber functionalism is in two

domains, namely "cyber functionalism for high political purposes (military geometric)" in the formulation and activation of cyber power to face the Global Cyber War (PSG), International Geometry War (PGA), and the complexity of the formation of the Cyber State or the Cyber Government; and "cyber functionalism for normal level political purposes (civil geometric)" in the form of protection of civil activity in cyberspace; 2) In order to prevent cyber crime, the implementation of the ID-SIRTII policy is integrated with the strategic role of national cyber institutions; 3) In order to face the Global Cyber Threat, the implementation of the ID-SIRTII policy needs to be integrated with regional and global cyber institutions; and 4) Departing from "cyber functionalism" and to create a structuralism of Indonesia's National Cyber Defense and Security, it is time for Indonesia to form a Cyber Force as a complement to the Army, Navy Agencies and Air Force.

Other previous studies conducted by Cahyadi (2016) entitled "Cyber governance and the threat to national sovereignty". The research objective is to understand the international debate on cyberspace governance and identify challenges in upholding sovereignty in cyberspace. Issues discussed in the research are mainly related to sovereignty in cyberspace, including the concept of sovereignty in cyberspace, challenges in the formation of cyberspace governance based on sovereign equality, as well as Indonesia's strategies in upholding sovereignty in cyberspace. The conclusion of the study states that China and the United States have applied the principles of sovereignty to guide global cyberspace governance, and therefore, Indonesia must immediately follow and act in an integrated manner in order to protect and safeguard its sovereignty in cyberspace efficiently.

The fifth previous research used as a reference for this research was conducted by Saputera (2015) entitled "The influence of the United States cyber security strategy in deaing with the threat of cyber warfare". The research objective is to study and describe the United States cyber security strategy in dealing with the threat of cyber warfare from 2009 to 2014. The type of the research is qualitative using secondary data collected from books, journals, articles, and from other valid sources on the internet. The results of the study stated that cyber warfare is a real threat, which can trigger physical warfare. The parties who carry out cyber attacks can enter the computer or network system without being able to be identified, to then dig up confidential data and use it for personal gain. Efforts made by the United States to deal with the threat of cyber war is by establishing a multi-functional intelligence agency, which can be an instrument of defense and security of cyberspace, as well as an instrument to launch cyber attacks.

III. RESEARCH METHODOLOGY

This research is a descriptive type with a qualitative approach. Descriptive research is a research that aims to describe a certain phenomenon systematically and accurately, to obtain detailed research findings (Silalahi, 2009). The qualitative approach is a research approach used to understand the focus of research based on data or information in the form of words or texts. Analysis of the data is carried out to gain a deep understanding on the focus of the study, so that an accurate interpretation can be made (Creswell, 2014). Therefore, the subjectivity of researchers in qualitative research has a significant role in determining the direction of data interpretation in order to answer the problem under study (Raco, 2013).

This study uses secondary data as the main material being analyzed. Secondary data obtained through the study of literature, namely by searching and gathering information relevant to the research topic (Silalahi, 2009). The data is then analyzed using qualitative analysis techniques consisting of three steps of analysis, namely data reduction, data presentation, and data interpretation. The first step, namely data reduction, is the step that determines the acquisition of the relevant data. This step is carried out by summarizing and grouping data based on their level of relevance to the research topic. The data used are only the high relevance one, whereas less relevant data will be ruled out. The second step after data reduction is the presentation of data, which is carried out to facilitate the researcher in observing and analyzing data, and to obtain a proper understanding of the data. The third and final step in qualitative analysis is the interpretation of data, which is carried out to obtain conclusions that answer the research objectives (Bungin, 2017).

IV. DISCUSSION

Development of national defense is essentially organized to be able to create a safe, peaceful and prosperous environment (Husain, 2019). According to Article 1 of the Law of the Republic of Indonesia Number 3/2002 concerning National Defense, efforts to realize those objectives include all efforts to maintain the country's sovereignty, the territorial integrity of the Unitary State of the Republic of Indonesia, and the safety of all nations from threats and disturbances to national integrity and country. These efforts are universal and are based on an awareness of the rights and obligations of citizens and a belief in one's own strength. The meaning of the universal efforts is to involve all citizens, territories and other national resources, and be prepared early by the government and carried out in a total, integrated, directed, and continuing manner to uphold the sovereignty of the country, territorial integrity, and safety of all nations from all threat.

The development of national defense becomes an increasingly urgent matter to be accelerated when there are indications of threats that actually have a widespread negative impact, which in the context of this study comes from cyber attacks. This is consistent with the risk matrix stated by Rahmawati (2017) which links the high risk of cyber crime and the need for defense development.

According to the risk matrix, the higher the risk caused by cyber threats, the more the need for accelerated development or increased national defense. The risk of cyber threats can be assessed based on two components, namely the probability component and the consequence component. The probability component refers to the possibility of future cyber attacks on the security of state confidential data. As stated earlier, the increasing number of internet users in the world in general, and in Indonesia in particular, is a core factor that makes the probability of cyber attacks on national defense even greater. This is also supported by data collected by BSSN, that during 2018 there were around 12 million cyber attacks on Indonesia. Thus, it can be stated that future cyber attacks have a high probability of occurring in far greater numbers than now.

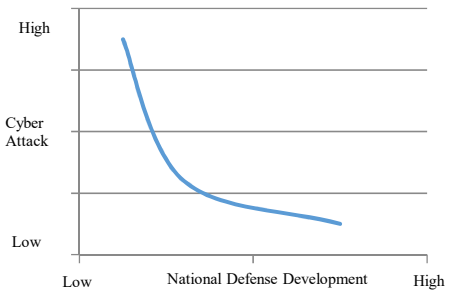


Figure 4. Risk Matrix
Source: Rahmawati (2017)

The consequences component refers to the negative impacts and damage caused by cyber attacks. As explained earlier, the global losses from cyber attacks in 2017 are estimated to have reached around eight thousand trillion rupiah (Franedya, 2018), whereas specifically for Indonesia, the cyber attack in 2018 had caused a loss of around four hundred trillion rupiah (Gewati, 2019). In addition, it is known that cyber attacks have three threat categories, namely hardware threats, software threats, and data/information threats, with the main target in the nine vital areas of human life which include health organizations, the public sector, educational institutions, individuals, finance, entertainment business, media, retail, and technology industries (McAfee.com, 2019). This shows that the impact and damage from cyber attacks has a very broad scope, so the consequences of cyber attacks will be felt by all levels of society. Based on this, both the probability and consequences of cyber threats can be said to be very large, which requires an acceleration in the development of national defense, especially those focused on dealing with various threats that come from the digital world.

Efforts to develop national defense forces in the context of overcoming cyber threats are carried out by the government by establishing its legal foundation, namely the Regulation of the Minister of Defense (Permenhan) of the Republic of Indonesia No. 82/2014 concerning Cyber Defense Guidelines and Presidential Regulation No. 53/2017 of the States Siber and Code Agency. Furthermore, there are also Government Regulation of the Republic of Indonesia No. 82/2012 concerning the Implementation of Electronic Transactions and Systems (PSTE) and Law of the Republic of Indonesia No. 19/2016 concerning Amendments to Law No. 11/2008 concerning Information and Electronic Transactions (ITE). There are also regulations that are in the formulation stage, namely

the Law on the Protection of Personal Data (PDP) and the Law on Cyber Security and Endurance (KKS)

The entire law, both those that have been established and those that are still in the process of formulation, are a reference in implementing efforts to overcome cyber threats that can originate from various sources. According to Permenhan No. 82/2014 concerning Cyber Defense Guidelines, there are at least nine sources of cyber threats, namely internal and external sources; intelligence activities; disappointment; investigation; extremist organization; hacktivist; organized crime groups; competition, hostility & conflict; and technology. All of these sources have the potential to create cyber threats ranging from Advanced Persistent Threats (APT), Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks, defacement, phishing, malware, cyber intrusion, spam, and abuse of communication protocols.

Various forms of cyber threats can increase in intensity and scale, until finally realized into cyber attacks in the form of actions or activities aimed at entering, controlling, modifying, stealing, and destroying a system or information asset. Broadly speaking, cyber attacks can be categorized into two, namely large-scale attacks in the form of cyber warfare and small-scale so-called cyber disruption. The impact resulting from cyber attacks can be in the form of functional disruption, remote control of the system, misuse of information or data, riots, fear, violence, chaos, conflict, and other adverse conditions that can lead to the destruction of the living order.

In order to overcome those threats and cyber attacks, the government formulated a framework for implementing cyber defense as outlined in Chapter IV Permenhan No. 82/2014 with components consisting of policies or regulations, institutions or organizations, technology and infrastructure, and human resources (HR). The policy or regulatory component consists of the legal basis of cyber defense, namely the Information and Electronic Transactions Law (ITE Law) No. 11/2008, Law No. 3 of 2002 concerning National Defense, Government Regulation of the Operator of Electronic Transactions and Systems (PP PSTE) No. 82/2012, and Minister of Defense Regulation No. 16 of 2010 concerning the Organization and Work Procedure of the Ministry of Defense. In addition there are also other policies, such as strategic policies, operational policies, information security management and their application, and standards that are used as a reference for cyber defense policies.

The institutional component refers to the institutions established by the government with the specific task of carrying out cyber defense. In accordance with Presidential Regulation of the Republic of Indonesia No. 53/2017 concerning the State Cyber and Code Agency, the institution established by the government as the organizer of cyber defense is the BSSN. The technology and infrastructure component refers to various technologies and infrastructure needed in the implementation of cyber defense. The components consist of infrastructure for building/location of data centers, NOCs, laboratories and other supporting facilities; Data Center and recovery center (Disaster Recovery Center/DRC); Data Network; Cyber defense administration application; Special applications for cyber defense; and special technology (hardware and software supporting specific cyber defense activities). The HR component refers to HR who have the competencies needed to carry out cyber defense, as well as HR recruitment methods and HR competency improvement programs. The stages of the implementation of cyber defense consist of the stages of attack prevention, the stage of monitoring information security, the stage of attack analysis, the stage of defense, the stage of counterattack, and the stage of enhancing information security.

As stated earlier, the main target of various cyber threats and attacks is the national important and confidential data. This is based on the position of data as the main asset in the digital age, where mastery of data is critical to the success of development in all fields, giving the greatest contribution in efforts to master various types of resources, as well as the main determinants of competitiveness that outperform other parties (Hummel et al., 2018). However, the matter of data and its sovereignty has not been made a top priority in the framework of the implementation of cyber defense as outlined in Permenhan No. 82/2014.

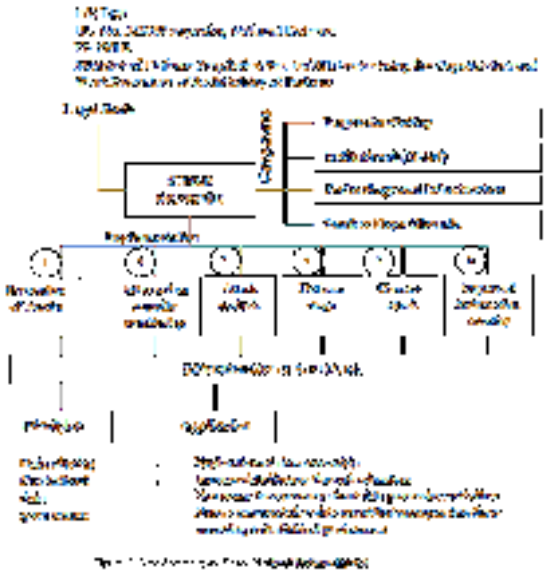
The sovereignty of the data stated implicitly in the Academic Paper on the Draft Law on Cyber Security and Resilience (KKS) in the review of cyber implementation in Indonesia. In that part, the term cyber sovereignty is mentioned, which describes the desire of the government to exercise control over the internet within its own territory, including political, economic, cultural and

technological activities. The ultimate goal of internet governance is to keep state confidential data safe from various cyber threats and attacks. Thus, the concept of data sovereignty basically also has similarities with cyber sovereignty, where the government will be positioned as a party that has full control over all data flows in the territory of the country of Indonesia. However, this concept is actually still being debated because of indications of violations of citizens' privacy due to government control over all data, including personal data of citizens.

According to Hummel et al. (2018), data sovereignty is the final goal to be achieved from the management of Communication and Information Technology. In this case, the data in an area is in the hands of the government of that region, so there are certain restrictions for the people in it. However, given the importance of data sovereignty in digital defense strategies to realize digital security and sovereignty, it is necessary to make efforts to make government authority and the limits given by the government for the use of data in its territory be accepted by the public, namely by regulating the principles and procedures for sharing data

Furthermore, data sovereignty can be applied by exploring data ownership, increasing data literacythrough education, encouraging transparency about data processing activities, and forming representative data agents that manage data flow according to individual preferences.

Based on the overall explanation above, the national defense model based on data sovereignty can be illustrated as follows:



V. CONCLUSIONS AND RECOMMENDATIONS

The government already has a cyber defense framework as outlined in Permenhan No. 82/2014 concerning Guidelines for Cyber Defense, which sets out the components along with the stages of the implementation of cyber defense. The first component is the regulatory or policy component consisting of the legal basis of cyber defense, namely the Information and Electronic Transactions Law (UU ITE) No. 11/2008, Law No. 3 of 2002 concerning National Defense, Government Regulation of the Operator of Electronic Transactions and Systems (PP PSTE) No. 82/2012, and Minister of Defense Regulation No. 16 of 2010 concerning the Organization and Work Procedure of the Ministry of Defense.

The second component is the institutional component that has been established through the establishment of the BSSN. The third component is the technology and infrastructure component which includes infrastructure for buildings/locations of data centers, NOCs, laboratories and other supporting facilities; Data Center and recovery center (Disaster Recovery Center / DRC); Data Network; Cyber defense administration application; Special applications for cyber defense; and special technology. The fourth component is HR along with HR recruitment methods and HR competency improvement programs.

Cyber defense is carried out in six stages, namely the attack prevention stage, the information security monitoring stage, the attack analysis stage, the defense stage, the counter attack stage, and the information security enhancement stage. Although data sovereignty has not been included in the framework of the implementation of defense, data sovereignty is essentially a basic foundation of national defense development to overcome threats and cyber attacks that have a high probability of occurring with massive consequences of damage.

Data sovereignty in the framework of cyber defense can be applied with reference to the principles of data sharing and centralization of data governance, with the application process including exploration of data ownership, increasing data literacy, encouraging transparency about data processing activities, and forming representative data agents that manage data flow accordingly with individual preferences.

The findings of this study can be considered by the government in the formulation of the concept of cyber defense by integrating data sovereignty as one of its basic components. This research can also be used as a reference for further researchers who want to re-examine the concept of data sovereignty in relation to national defense development in the digital age.

VI. REFERENCES

Arianto, A. R., & Anggraini, G. (2019). Membangun Pertahanan Dan Keamanan Siber Nasional Indonesia Guna Menghadapi Ancaman Siber Global Melalui Indonesia Security Incident Response Team On Internet Infrastructure (ID-SIRTII). *Jurnal Pertahanan & Bela Negara*, *9*(1), 13–29.

Gultom, R., Midhio, W., Silitonga, T., & Pudjiatmoko, S. (2018, March). Introducing the Six-Ware Cyber Security Framework Concept to Enhancing Cyber Security Environment. In ICCWS 2018 13th International Conference on Cyber Warfare and Security (p. 262). Academic Conferences and publishing limited.

Parks, R. C., & Duggan, D. P. (2011). Principles of cyberwarfare. IEEE Security & Privacy, 9(5), 30-35.

BSSN. (2018). *2018 Honeypot project BSSN-IHP*. Jakarta Selatan.

Bungin, B. (2017). *Metodologi Penelitian Kuantitatif*. Jakarta: PT Fajar Interpratama Mandiri.

Cahyadi, I. (2016). Tata Kelola Dunia Maya Dan Ancaman Kedaulatan Nasional. *Politica*, *7*(2), 210–232.

Creswell, J. W. (2014). *Research Design: Quantitative and QUalitative APproach*. London: Sage Publishing.

Craswell, J.W. (2018). Research Design; Qualitative, Quantitative and Mixed Methods Approaches. London: SagePublication

Crotty, M. (1998). The Foundations of Social Research: Meaning and Perspective in the Research Process. London: SagePublication

Denzin, NK. dan Lincoln, YS. (2018). Sage handbook of Qualitative Research, London: SagePublication

Bernard, HR. (2006). Research Methods in Antropology. Qualitative and Quantitative Approaches. Toronto: Altamira

MTAN. (2018). Materi Trilogi Penelitian Sosial. Surabaya: MTAN

Tracy, SJ. (2013). Qualitative Research Methods. UK: Wiley Blackwell.

Taylor, SJ, Bogdan, R., and DeVault, ML. (2016) Qualitaive Research Methods, UK: Wiley Blackwell

Taylor, PC., and Wallace, J. (2017). Qualitative Research in Postmodern Times. Netherlands: Springer

Franedya, R. (2018). Kerugian Akibat Kejahatan Siber Mencapai Rp 8.160 T/Tahun. Retrieved from www.cnbcindonesia.com website: https://www.cnbcindonesia.com/tech/20180222063411-37-5062/kerugian-akibat-kejahatan-siber-mencapai-rp-8160-t-tahun

Gewati, M. (2019). RI Rugi Rp 478,8 Triliun akibat Serangan Siber, DPR Siapkan RUU KKS. Retrieved from nasional.kompas.com website: https://nasional.kompas.com/read/2019/08/12/13454311/ri-rugi-rp-4788-triliun-akibat-serangan-siber-dpr-siapkan-ruu-kks?page=all

Hummel, P., Braun, M., Augsberg, S., & Dabrock, P. (2018). Sovereignty And Data Sharing. *ITU Journal*, *2*(23).

Husain, A. (2019). *Ketahanan dasar lingkungan*. Makassar: CV Sah Media.

Jazuli, A. (2016). Pembangunan Pertahanan Dan Keamanan Demi Penegakan Hukum Di Indonesia: Kewibawaan Suatu Negara. *Jurnal Penelitian Hukum*, *16*(2), 187–199.

McAfee.com. (2019). *McAfee labs threats report*. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

Prasetia, A. (2019). Jokowi: Lindungi Kedaulatan Data Tanpa Kompromi, Siapkan Regulasi! Retrieved from news.detik.com website: https://news.detik.com/berita/d-4667990/jokowi-lindungi-kedaulatan-data-tanpa-kompromi-siapkan-regulasi

Raco, J. R. (2013). *Metode penelitian kualitatif*. Jakarta: Grasindo.

Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) Dalam Peningkatan Cyber Defense. *Jurnal Pertahanan & Bela Negara*, *7*(2), 51–66.

Rizal, M., & Yani, Y. M. (2016). Cybersecurity Policy and Its Implementation in Indonesia. *Journal of ASEAN Studies*, *4*(1), 61–78.

Saputera, M. Y. (2015). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare. *JOM FISIP*, *2*(2), 1–

14.

Silalahi, U. (2009). *Metode Penelitian Sosial*. Bandung: PT. Refika Aditama.

Tedyyana, A., & Supria. (2018). Perancangan Sistem Pendeteksi Dan Pencegahan Penyebaran Malware Melalui SMS Gateway. *Jurnal Inovtel Polbeng*, *3*(1), 34–40.

European Commission. A Digital Single Market Strategy for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Available online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX: 52015DC0192 (accessed on 20 November 2018).

Bundesministerium für Verkehr und digitale Infrastruktur. Eigentumsordnung für Mobilitätsdaten? Eine Studie aus technischer, ökonomischer und rechtlicher Perspektive. Published in 2017. Available online: https: //www.bmvi.de/SharedDocs/DE/Publikationen/ DG/eigentumsordnung-mobilitaetsdaten.html (accessed on 20 November 2018).

Smart City Charter: Making digital Transformation at the Local Level Sustainable. Scientific Support: Federal Institute for Building, Urban Affairs and Spatial Development (BBSR), Division I 5—Digital Cities, Risk Prevention and Transportation, Stephan Günthner. Available online: https : // www.bbsr.bund.de / BBSR / EN / Publications / SpecialPublication / 2017/smart-city-charta-de-eng.html (accessed on 20 November 2018).

Die Bundesregierung (The German Gouvernement). Deutsche Nachhaltigkeitsstrategie— Neuauflage. 2016.Available online: https://www.bundesregierung.de/Content/Info material/BPA/Bestellservice/Deutsche_Nachha ltigkeitsstrategie_Neuauflage_2016.pdf?__blob =publicationFile&v=23 (accessed on 20 November 2018).

Schieferdecker, I.; Bruns, L.; Cuno, S.; Flügge, M.; Isakovic, K.; Klessmann, J.; Kraft, V.; Lämmel, P.;Stadtkewitz, D.; Tcholtchev, N.; et al. Urbane Datenräume—Möglichkeiten von Datenaustausch undZusammenarbeit im Urbanen Raum. pp. 1–275, Published in June 2018. Available online: https://cdn0.scrvt.com/fokus/774af17bdc0a18cd/69f7a401c168/UDR_Studie_062018.pdf (accessed on 20 November 2018).

Greater London Authority. Data for London: A City Data Strategy. 2016. Available online:https://files.datapress.com/london/dataset/data-for-london-a-city-data-strategy/2016-03-01T09:46:23/London%20City%20Data%20Strategy%20March%202016.pdf (accessed on 21 November 2018).

PwC Study. Datenaustausch als wesentlicher Bestandteil der Digitalisierung. 2017. Available online:https://www.pwc.de/de/digitale-transformation/studie-datenaustausch-digitalisierung.pdf (accessed on22 November 2018).

Schwerpunktinitiative Digitale Information der Allianz der deutschenWissenschaftsorganisation— Forschungsdaten.Available online: https://www.allianzinitiative.de/de/archiv/forschungsdaten (accessed on 22November 2018).

Deutsche Forschungsgemeinschaft. Leitlinien zum Umgang mit Forschungsdaten. Available online: http://www.dfg.de/download/pdf/foerderung/antragstellung/forschungsdaten/richtlinien_forschungsdaten.pdf (accessedon 22 November 2018).

Kuzev, P.;Wangermann, T. Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht; Konrad-Adenauer-Stiftung e.V.: Berlin, Germany, 2018.