LESREV (Lex Scientia Law Review), **E-ISSN: 2598-9685 , P-ISSN: 2598-9677**
Vol. 4 ***No.*** 1 ***Month*** May ***Year 2020***

Critical Review of The Urgency of Strenghthening The Implementation of Cyber Security and Resilience in Indonesia

Indirwan, Sarah Safira Aulianisa
[1]Faculty of Law, Sebelas Maret University, [2]Facultu of Law, Indonesia University
Jl. Ir Sutami No. 36A, Surakarta, Jawa Tengah 57126, Jl. Prof. Mr Djokosoetono, Depok City, West Java 16424

Article Info: Submitted April 8, 2020 Accepted April 26, 2020
Published May 9, 2020

Abstracts :
The development of information technology in cyberspace is unavoidable. Which followed by the vulnerability of threats and attacks on data and information traffic that can threaten the country's sovereignty. One of the ways that can be done is to strengthen Indonesia's cyber infrastructure and institutions. The purpose of this legal research is to find out the urgency of regulating Cybersecurity and resilience in Indonesia and its challenges and obstacles, also to conduct a comparative study in several countries. This research is a normative legal research with qualitative descriptive analysis. The results of the study indicate that arrangements regarding Cybersecurity and resilience are very important and must be enacted immediately.
Keyword : *Threats and Attacks; Security and Resilience; Cyber, Urgency.*

Vol. 4, No. 1
Month May **Year** 2020

Abstrak :
Perkembangan teknologi informasi dalam ruang siber merupakan hal yang tidak dapat dihindari. Hal ini diikuti dengan rentannya ancaman dan serangan terhadap lalu lintas data dan informasi yang dapat mengancam kedaulatan negara. Salah satu upaya yang dapat dilakukan adalah dengan melakukan penguatan infrastruktur dan kelembagaan siber Indonesia. Tujuan penelitian hukum ini untuk mengetahui urgensi pengaturan keamanan dan ketahanan siber di Indonesia beserta tantangan dan hambatannya, serta melakukan studi komparasi tentang penyelenggaraan keamanan dan ketahanan siber di beberapa negara. Penelitian ini merupakan penelitian hukum normatif dengan analisis deskriptif kualitatif. Hasil penelitian menunjukkan pengaturan mengenai keamanan dan ketahanan siber sangatlah penting dan harus segera dinormatifikasi.
Kata Kunci : *Ancaman dan Serangan; Keamanan dan Ketahanan; Siber, Urgensi.*

Citation :
Indirwan, Sarah Safira Aulianisa. (2020). Critical Review of the Urgency of Strengthening the Implementation of Cybersecurity and Resilience in Indonesia Lex Scientia Law Review 4(1), 33-48. doi: https://doi.org/10.15294/lesrev.v4i1.38197

1. Introduction

In the era of globalization accompanied by increasingly rapid advances in science and technology, the existence of information has meaning and important roles in all aspects of life. In today's modern society, information has functioned like the flow of blood which is the source of life for the human body[1]. At present, many countries have a high dependence on cyberspace and the internet, both in economic, business, social, political, government, defense, and security aspects. Cyberspace is a space in which communities are connected using networks (for example the internet) to carry out various daily activities (Ministry of Defense of the Republic of Indonesia, 2014). This development, on the one hand is a necessity that is beneficial because it can support economic development and relations between countries. Through constructive use of cyberspace, social relations between nations can be held in a relatively short time without the constraints of space and time. But on the other hand, increased connectivity in cyberspace and dependence on the internet also pose a threat to state sovereignty with the possibility of cyber-based transnational crime. These threats can come from governments, organizations, individuals, or entrepreneurs, whether intentionally or not to gain financial, military, political, or other benefits[2].

Along with the times, the sovereignty and resilience of a country is not only judged by how much military or economic power it has, but also depends on aspects of mastery, use, and empowerment of cyberspace. Indonesia also faces global challenges related to national security and resilience in cyberspace. This challenge can have implications for new threats, for example in the form of cyberattacks, cybercrime, cyber prostitution, cyber propaganda, cyber terrorism to cyber warfare. The nature and characteristics of cyberspace that are borderless, spaceless, and timeless, make cybercrime a form of transnational crime[3]. In the Strategic Study of National Cybersecurity, the threat of cybercrime is defined as any condition and situation as well as the ability that is considered capable of carrying out actions or disruptions or attacks that are capable of damaging or anything detrimental so that it threatens confidentiality, integrity and availability of systems and information[4]. In this context, based on the 2017 Global Cybersecurity Index (GCI) report released by The UN International Telecommunication Union (ITU), Indonesia is among countries with weak Cybersecurity. Of the 195 countries, Indonesia ranks 70th with a score of 0.424. The first rank of the country with the best Cybersecurity is Singapore, followed by the United States in second place, and Malaysia with a score of 0.893 in the third rank[5].

If viewed from the rise of cybercrime that occurred, followed by the inclusion of Indonesia in the ranking of countries with weak Cybersecurity, then there has actually been an urgency to develop security and resilience strategies in cyberspace. In contrastto other crime subscriptions, Cybersecurity and security requires

---

[1] Brascomb, A. W. (1986). *Toward A Law of Global Communication Network.* New York: Lognman, p. 16

[2] Smith, M. (2015). *Research Handbook on International Law and Cyberspace*. Massachusetts: Edwar Elgar Publishing Limited, p. 28

[3] Gultom, R. A. (2017). Membangun Kemampuan Siber dan Persandian Nasional guna Mengantisipasi Tantangan Keamanan Siber di Era Globalisasi Informasi dalam Rangka Melindungi Keutuhan dan Kedaulatan NKRI,. *Jurnal Kajian Lemhanas*, 30(12), p. 28

[4] Kustiyawan, I. (2012). *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber*. Tesis Universitas Pertahanan Indonesia, p.22.

[5] Badan Siber dan Sandi Negara. (2018). *Indonesia Cybersecurity Monitoring Report.* Jakarta: BSSN, p. 12

comprehensive thinking in forming its policies by the Government. A comprehensive approach is needed as well as comprehensive studies with other countries in order to realize strong and well-integrated national Cybersecurity and security institutional arrangements and arrangements. The implementation of Cybersecurity in Indonesia is still experiencing problems because it has not become a coordinated national initiative. The implementation step is still sectoral and based on interests, capabilities, and deterrence as well as its mitigation and recovery is also still weak, so that it is still very vulnerable to massive attacks. Based on these matters, this paper aims to conduct a critical review of the urgency of the ratification of the Draft Bill on Cybersecurity and Resilience in order to provide a legal umbrella for the implementation of Cybersecurity strategies in Indonesia, conduct comparative studies on security arrangements and cyber resilience in other countries, as well as to find out the challenges and obstacles in the framework of the establishment and ratification of the Draft Bill on Cybersecurity and Resilience in Indonesia.

Problem Formulation

Based on this background, the Author formulates several issues as the focus of this study, which is how is the urgency of strengthening the implementation of cybersecurity and resilience in Indonesia? How is the implementation of cybersecurity and resilience in other countries? and how are the challenges and obstacles in strengthening the implementation of Cybersecurity and resilience in Indonesia? With the formulation of the problem, this legal research is intended as a comprehensive solution to address the issue of Cybersecurity and resilience that could threaten the country's sovereignty in the future.

2. Research Methods

The type of research that the Author uses is normative legal research or commonly known as doctrinal law research which is commonly referred to as legal research or legal research instruction. This legal research examines the literature material obtained through literature study by collecting and studying primary and secondary legal materials in the form of legislation and literature relevant to the object of research. The approach used in this legal research is the statute approach and the conceptual approach. The statute approach is carried out by examining all laws and regulations relating to the legal issues being studied. The conceptual approach is carried out by analyzing and examining the urgency of regulations regarding Cybersecurity and resilience in Indonesia. The analysis used is descriptive, which is to describe or explain the phenomenon under study. Analysis is done by linking cause and effect to the emergence of the phenomenon under study.

3. Result and Discussion

3.1 Construction of Cybersecurity and Resilience in Indonesia

3.1.1 Status Quo and Development of the Implementation of Cybersecurity and Resilience in Indonesia

The implementation of cybersecurity and resilience practiced in Indonesia is on a national scale that is still scattered in various government institutions or agencies such as the Ministry of Defense and the Indonesian National Police. This is due to the absence of a positive law that specifically regulates the phenomena of cybersecurity and resilience and the implementation of cybersecurity and resilience has not been integrated and integrated. In Indonesia, the regulations

are still very limited and have weaknesses in protecting cyber infrastructure. Some of the regulations currently related to cybersecurity include The Act Number 32 of 2002 on Defense, The Act Number 34 of 2004 on TNI, The Act Number 43 of 2008 on State Territories. Regulations that are used as a legal umbrella for this problem, for example, refer to the Law on Information and Electronic Transactions and Government Regulations on the Implementation of Electronic Transactions and Systems. However, this law is unable to cover the handling of tapping (interception) practices in cyberspace or e-commerce governance and has not been able to reach all aspects of Cybersecurity that are so broad.

In addition, The Act Number 36 of 1999 on Telecommunications, The Act Number 32 of 2002 on Broadcasting, and The Act Number 14 of 2008 on Openness of Public Information, still has limitations in the context of telecommunications, broadcasting and informatics infrastructure for public services. Existing government regulations also do not regulate the role of government in the security system and cyber resilience, so that its use for Cybersecurity is still very limited. One of the government's efforts in dealing with cyber threats and attacks can be seen from the existence of The Ministerial Regulation Number 82 of 2014 concerning Cyber Defense Guidelines, but these guidelines are prepared as a reference for the stages of preparation, development, implementation and stabilization of cyber defense only in the environment of the Ministry of Defense and TNI. Then, in The Act Number 17 of 2011 on Intelligence also has limitations to conduct cyber espionage as well as to carry out limited Cyberattack responses.

In 2017, the National Siber and Coding Agency (BSSN) was officially established by the Government which is under and is responsible to the President through ministers who coordinate, synchronize, and control governance in the political, legal and security fields. BSSN has the duty to implement Cybersecurity effectively and efficiently by utilizing, developing, improving, and consolidating all elements related to security cyber (The Ministry of Communication and Information Technology Republic of Indonesia, 2019). Then this body aims to protect national cyber activities without violating the rights of individuals or companies in the use of the internet, so it is clear that this body will not interfere in the private domain of internet users. However, due to the lack of specific regulations, coordination between agencies has not been effective and still works according to the guidelines of their respective institutions. The practice of providing security and cyber resilience can be seen in the body of the Ministry of Defense. The Ministry of Defense established a Cyber Defense Center (Pushansiber) that has the task of carrying out governance, cooperation, operations, and guarantees of cyber defense. Pushansiber is active in the annual international security forum that focuses on cyber working groups and is also involved in various focus group discussions on cyber and data sovereignty.

Furthermore, TNI under the Ministry of Defense has formed a Cyber Unit (Satsiber) to carry out cyber defense activities and operations. Existing Satsiber is a task force organization tasked with carrying out cyber activities and operations within the TNI AD in order to support the main tasks of the TNI AD. Existing Satsiber has become a work unit that has a function as monitoring and defense in facing Cyberattacks and crime as well as providing quick responses and

reporting to the leadership of the TNI AD in order to secure the TNI AD institutions from threats of crime and Cyberattacks. There are four functions that are owned by the Satsiber TNI, that are detection, protection, recovery and ensuring that the existing cyber system has no holes or deficiencies that can be entered by malware or backdoor. Moreover, in the body of the Indonesian National Police there is the Directorate of Cyber Crimes (Dittipidsiber) which is under the Criminal Investigation Police with a focus on the task of conducting law enforcement against cybercrime which is generally divided into computer crime and computer-related crime. The forms of crime are hacking of electronic systems, illegal interception, web defacement, system interference, and data manipulation. Second, cyber crime that uses computers as a tool, such as online pornography, online gamble, online defamation, online extortion, online fraud, hate speech, online threat, illegal access, and data theft.

The State Intelligence Agency (Badan Intelijen Negara) has also formed a Deputy Cyber Siber which has the duty to support the performance of BIN in inadequate intelligence work if it relies only on human intelligence and must be strengthened with cyber intelligence. The existence of the deputy carries out the functions of preparing plans for cyber intelligence activities and/or operations, carrying out cyber intelligence activities and/or operations, coordinating cyber intelligence activities and/or operations, controlling cyber intelligence activities and/or operations, and preparing cyber intelligence reports.

In response to the cyberattack, the Ministry of Communication and Information has formed a team called ID-SIRTII/CC (Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center) to ensure internet security in Indonesia. ID-SIRTII/CC was formed with the aim of supporting the implementation of the law enforcement process, creating an environment and utilization of internet protocol-based telecommunications networks that are safe from various threats and disturbances, and supporting the implementation of coordination with related parties both inside and outside the country in prevention efforts, detection, early warning and incident mitigation on strategic infrastructure. ID-SIRTII/CC has attempted to monitor national internet anomaly traffic from January to December 2018, as many as 232,447,974 Cyberattacks have been found on the Indonesian network.

3.1.2 Non-Litigation Pathway

The cyberspace phenomenon illustrates a reality that the activities of modern society are now connected through cyberspace and the internet. Geopolitical discourse is becoming increasingly complex given the world is currently entering the phase of the Fourth Industrial Revolution. In this new industrial order, artificial intelligence (AI), internet of things (IoT), big data, cloud, and mobile technology change the economy, industry, and life of world citizens in a very fundamental way[6]. From the perspective of cybersecurity and resilience, the use of the internet is also possible for negative or destructive purposes by various parties who have the ability, whether done individually, in groups (non-state actors) to a country (state actors).

[6] Soepandji, K.W & Farid, M. (2018). Konsep Bela Negara dalam Perspektif Ketahanan Nasional,. *Jurnal Hukum dan Pembangunan*, 48(3) p. 442.

The Act Number 3 of 2002 on National Defense states that national defense is carried out through efforts to build and foster the ability, deterrence of the state and nation, and overcome any threats. In this context, the Indonesian people need a resilience to National Resilience, that is the dynamic condition of the Indonesian nation which covers all aspects of national life that are integrated and contains resilience and resilience that contains the ability to develop national strength in facing and overcoming all challenges, threats, obstacles and disturbances, both coming from outside and from within, to guarantee the identity, integrity, survival of the nation and state, and the struggle to achieve their national goals[7].

Cyberspace in various countries is considered as a vital thing, because there is a threat to the rotation of information that can affect the stability of a country. In the era of globalization, threats to a country are not only intended to attack government or military agencies but can threaten all aspects of people's lives, such as the economy, politics, culture, and security of a country. This technological transformation causes the threats faced by a nation to become more complex. The pattern of battle and the strategies used have changed and shifted from. Conventional or asymmetric warfare methods, to asymmetric warfare[8]. In modern warfare, it has begun to abandon the forms and patterns of traditional or conventional warfare administrative, technical, and ideological.

Some national security and defense threats are carried out by non-state actors, such as terrorism, insurgency, cybercrime, human trafficking, piracy, drug trafficking, and even including violations of human rights (human rights). In this asymmetrical warfare conflict, it is carried out by non-state actors as a weak party against the Government as a strong party or how a weak state against a strong state[9]. In conventional warfare, enemies, state actors, troops, and military equipment are all clearly seen. In contrast to asymmetrical warfare, all of which are in a virtual or intangible context. Asymmetrical warfare can be carried out indirectly, aiming to influence strengths and exploit the weaknesses of opponents by utilizing technology and public unrest.

Regarding asymmetric warfare, Richard Clarke defines cyber warfare as an action by the nation-state to penetrate other nation's computers or networks to cause damage or disruption[10]. Meanwhile, Andi Hamzah in his book "Criminal Aspects in the Field of Computers", defines computer crime as a crime in the computer field in general that can be interpreted as the illegal use of computers, as well as basing the types of cyber crime activities as follows[11] :

1. Unauthorized Access to Computer System and Service. Crimes by breaking into a computer network system illegally or without permission. The perpetrators of the crime (hackers) sabotage or theft of important information;

---

[7] Ibid

[8] Dorman Andrew, S. M. (2002). *The Changing Face of Military Power: Joint Warfare in an Expeditionary Era (Cormorant Security Studies Series).* London: Palgrave Macmillan, p. 33

[9] T Franklin D.& Kramer. (2009). *Cyberpower and National Security* . Washington Dc: National Defense University, p. 26

[10] Clarke, R. A. (2010). *Cyber War: The Next Threat to National Security And What To Do About It.* . New York: Harper Collins, p.44

[11] Hamzah, A. (1990). *Aspek-aspek Pidana di Bidang Komputer.* Jakarta: Sinar Grafika, p. 27

2. Illegal Contents. Crimes by entering data information through the internet about something that is not true, unethical, disturbing public order, and breaking the law. An example is loading hoax or slander that can destroy the reputation of another party;
3. Data Forgery. Crimes committed by falsifying data on important documents stored through the internet;
4. Cyber Espionage. Crimes in utilizing the internet network by entering a computer network system (computer network system) to be able to spy on other parties;
5. Cyber Sabotage and Extortion. Crimes committed by making interference, destruction or destruction of data, computer programs or computer network systems connected to the internet;
6. Cracking. The crime of using computer technology to damage a computer security system and to steal it once you get access;
7. Cybercrime Against Government. Crimes that have a specific purpose to attack government.

With the development of technology, many countries are changing defense strategies towards capability-based or scenario-based defense strategies. This approach provides flexibility and can face the future. Strategies that are only based on current threats will always be left behind and there is not enough time to make changes or adjustments without risk[12]. The defense aspect must also pay attention to defense or military technology. The development of defense technology not only gives greater strength, but the most important thing is to change the way of war and defense, which also means forming a defense strategy. Security strategies and systems are not static but dynamic in nature, in which security system changes are strongly influenced by the dynamics of a strategic environment that continues to evolve and continue to change.

3.2 Urgency of Regulation for the Implementation of Cybersecurity and Resilience in Indonesia

3.2.1 Draft Bill on Cybersecurity and Resilience for National Sovereignty and Defense

Conflict and competition in cyberspace is part of a larger movement in the international security environment. According to James R. Langevin, when the use of cyberspace has increased, likewise the misuse of cyberspace space[13]. Thus, the higher the level of dependence of the Government and the community of a country on a technology, then at the same time the greater the threat by using that technology to society and the country's sovereignty. Likewise with the progress of internet technology which is now almost able to connect all dimensions of human life in the cyber world. Indonesia, as one of the countries with an increasing number of internet users every year, shows that the use of cyberspace in Indonesia has a big opportunity as well as a threat.

Based on the results of national internet anomaly traffic monitoring from January to December 2018, there were 232,447,974 Cyberattacks on the Indonesian network. Web network monitoring results found 16,939 cases of website incidents (defacement) with the most targeted domains being the go.id

[12] Prasetyono, E. (2008). Strategi Pertahanan Indonesia di Masa Depan. *Jurnal Analisis CSIS*, 37(3), p. 127.

[13] James R. & Langevin, M. T. (2011*). Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* . Washington DC: Center for Strategic and International Studies, p. 111

domain. The biggest threat to Indonesia this year is the threat of malware whose activity has been recorded at 122 million this year[14]. Then, based on the results of national anomaly traffic monitoring from January to December 2018, there were 232,447,974 attacks.

Throughout 2018, ID-SIRTII also conducted monitoring related to information security holes on the .id domain-based website. Obtained from the results of monitoring as many as 1,872 websites have security holes. The top 5 domains found for security holes are .co.id, .ac.id, .go.id, .sch.id, and .or.id. The security gap found is indicated to be exploited further[15]. Data leak monitoring in 2018 obtained data leakage of 785,967 from domains and records. The number consists of 785,906 records / lines from 61 various .id domains. Domains obtained by data leakage (data leakage) are .sch.id, .ac.id, .co.id, .or.id, .go.id, and .web.id domains[16].

Besides, the following are some examples of major cases of Cyberattacks or cyber warfare that have occurred by attacking or targeting a country's national interests, as follows[17]:

1. In 2007 at Estonia and 2008 at Georgia, Cyberattacks with the Distibuted Denial of Services (DDoS) attack on the two countries resulted in the paralysis of national critical infrastructure. Many observers believe the case of Estonia and Georgia as the first form of cyber warfare in the world. In Estonia, 2 (two) Internet Exchange nodes and fiber optic channels coming out of Estonia were intentionally shut down, causing huge state losses, while in Georgia, critical national infrastructure was paralyzed for several months. As a result of massive attacks and the resulting impact then inspired the preparation of international norms of cyber warfare as stated in the book Tallin Manual.
2. On August 2012 in Saudi Arabia, the Cyberattack incident using Shamoon Malware succeeded in damaging and destroying sensitive data of the Saudi Aramco Oil Company and infecting around 30,000 workstations or 75% of the company's total workstations.
3. On October 2016 in the United States, the United States Government "accused" the Russian party of carrying out a political hacker attack related to the 2016 US Presidential election. Parties involved direct electronic voting (electronic votes) in the United States, although this has been denied by the Russians. A valuable lesson to be learned from this case is the need for special attention to high Cybersecurity for the implementation of the Presidential Election or the elections using the electronic votes system. The role of the coding system (cryptography) is crucial in this aspect.

Various threats to Cybersecurity and resilience, especially in Indonesia, one of which is caused by the handling of cyber crime that is still partial and scattered and lack of standard coordination in handling Cybersecurity issues. Nationally,

[14] ID-SIRTII. (2018). *Laporan Tahunan.* Jakarta: ID-SIRTII.

[15] Ibid

[16] ID-SIRTII. (2018). *Indonesia Cybersecurity Monitoring Report 2018.* Jakarta: Desember

[17] Gultom, R. A. (2017). Membangun Kemampuan Siber dan Persandian Nasional guna Mengantisipasi Tantangan Keamanan Siber di Era Globalisasi Informasi dalam Rangka Melindungi Keutuhan dan Kedaulatan NKRI. *Jurnal Kajian Lemhanas*, 30(3), p. 28.

according to Hasyim Gautama there are several problems related to the development of robust Cybersecurity including[18] :

1. Lack of understanding of the management of the state or security related to the cyber world that requires restrictions on the use of services whose servers are abroad and the need for the use of a secured system.
2. The legality of handling attacks in the cyber world.
3. The pattern of cybercrime events is very fast so it is difficult to handle.
4. National cybersecurity institutional governance.
5. Low awareness of the threat of international cyberattacks that can paralyze a country's vital infrastructure.
6. Our industry is still weak in producing and developing hardware related to information technology which is a gap that can strengthen and weaken defenses in the cyber world.

Cybersecurity and resilience is one area of government that needs to be encouraged and strengthened as an effort to increase national economic growth and realize national security. Building strong national cybersecurity and resilience is inseparable from the role and cooperation of the military by maximizing all national components formed in civil-military cooperation. The realization of this is done by rearranging Government policies by utilizing, developing, and consolidating all elements related to Cybersecurity. In this case, the Government needs to make strategic policies in the form of certain regulation that can be used as guidelines or legal umbrella in implementing and supporting national defense in the field of Cybersecurity and resilience. With the existence of the legality of the national Cybersecurity strategy policy, it is expected to be able to realize the implementation of good national Cybersecurity to protect citizen information, law enforcement, and maintain the security and sovereignty of Indonesia from various existing threats.

3.3.2 Institutional Strengthening of The National Cyber and Encryption Agency (BSSN)

The existence of BSSN which was formed based on Presidential Regulation Number 53 of 2017 became a strategic step to increase the country's power in facing threats and Cyberattacks in Indonesia. The paradigm of the implementation of Cybersecurity and resilience must be formulated in a legal framework by prioritizing the coordinative and collaborative principles between the relevant stakeholders. The presence of BSSN is interpreted as a body that becomes the leading sector so that it can synergize various stakeholders effectively and efficiently. Strengthening BSSN by making it a leading sector strives so that the authority it will have does not overlap with the authority that has been held by various stakeholders today.

Institutionally, the BSSN which is a revitalization of the National Cryptographic Agency (Lembaga Sandi Negara) is not intended to be the sole organizer, thereby eliminating the functions and authority that each state agency has in place for Cybersecurity today. The presence of BSSN must be interpreted that in facing threats and crime in the cyber world, it needs a body that can

[18] Gautama, H. (2020). Cybersecurity. Retrieved from : http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, Accessed on 8 April 2020.

synergize various stakeholders to realize national security. Implementation of the existing authority in the body of BSSN must be able to realize Cybersecurity effectively and efficiently by utilizing, developing, and consolidating all elements related to Cybersecurity. To increase support for Cybersecurity and resilience, BSSN can work with local governments to create synchronization and uniformity in the implementation of Cybersecurity and resilience.

As a supporting component, public involvement is an important thing to do in order to support the implementation of Cybersecurity and resilience. The society is expected to unite themselves into an organization to participate in being a provider of Cybersecurity and resilience by utilizing the development of innovation in the fields of science and technology. The establishment of BSSN will increase the potential for professional human resource development in the field of Cybersecurity in Indonesia. In the context of cyber human resources, BSSN has the potential to develop cyber human resources that are professional and adaptive to technology for both internal and national needs. The existence of BSSN is expected to be able to meet the needs of cyber human resources who master information technology that continues to grow rapidly in Indonesia.

As for the context of performance, BSSN has the potential to build a performance management system that provides opportunities and rewards for innovations in the field of Cybersecurity in Indonesia. BSSN can build culture and behavior to improve productivity and professionalism of human resources in the field of Cybersecurity by initiating awards in the field of Cybersecurity for various organizations, both government and private, and even at the individual level.

3.3 Comparative Study of the Implementation of Cybersecurity and Resilience in Other Countries

The development of the rise of crime that occurs in cyberspace is something that must be anticipated because it can threaten the defense and sovereignty of a country. One of the efforts made by the Government to support this is by formulating Draft Bill on Cybersecurity and Resilience in the 2019 National Legislation Program. In the process of drafting the bill, comparative studies can be conducted with several countries that have set various computer crimes that can interfere with the administration of a government the state, business activities, the lives of people and individuals who can threaten national security and defense in the cyber field. Based on the Kaspersky Cybersecurity Index report, it shows that Indonesia's Cybersecurity is still far behind compared to other countries. The data in the report shows a description of the position of countries regarding the level of danger of use exposed online. In 2017, at the Asia and Pacific level, Indonesia's Cybersecurity index ranked 19. While other ASEAN countries rank better such as Singapore (6), Brunei Darussalam (8), Malaysia (9), Thailand (10), Philippines (15), and Vietnam (17).

Singapore is one of the countries in Southeast Asia based on the Global Security Index released by the International Telecommunications Union in 2017 categorized as the country with the first position on Cybersecurity compared to other countries in the world. In Singapore there is a Cybersecurity Agency of Singapore (CSA) as a Singapore government body under the Prime Minister's Office, but is administratively managed by the Ministry of Communication and

Information which provides centralized oversight of the national Cybersecurity function and enhances the security and resilience of Singapore's critical information infrastructure sector, working with the public and private sectors, focuses on protecting essential services in Singapore, such as in the energy and banking sectors. CSA consists of a Commissioner, Deputy Commissioner, and also Assistant Commissioner whose job is to carry out CSA functions.

In Australia, there is the Australian Cybersecurity Center (ACSC) which is responsible for Cybersecurity including analyzing, investigating and reporting cyber threats and coordinating national security capabilities and operations for incidents of cyber crime, cyberterorrism and cyberwarfare. ACSC is organized by the Australian Signal Directorate and in collaboration with the Australian Security Intelligence Organization led by a National Cyber Coordinator, which is overseen by the Cybersecurity Operations Council and is a joint responsibility of the Minister of Defense and the Minister of the Interior. ACSC also integrates national Cybersecurity capabilities throughout Cybersecurity missions with a number of institutions such as the strategic intelligence analyst of the Defense Intelligence Organization, the Domestic Computer Emergency Response Team, the Australian Federal Police Cyber Crime Investigator, and the Australian Criminal Intelligence Commission of cyber crime intelligence specialists. In addition there is also the National Cyber Coordinator whose job is to ensure effective partnerships both with non-governmental organizations, the private sector, and the research community as well as international partners to support the implementation of Cybersecurity and resilience.

Furthermore, in United States of America (USA), a National Cybersecurity Center (NCC) was formed which is part of the United States Department of Homeland Security is a national-level non-profit organization that provides collaborative cybersecurity knowledge and services to the nation. In addition, the National Cybersecurity Center of Excellence (NCCoE) was established, which is a United States government organization that builds and publicly shares solutions to Cybersecurity problems faced by US businesses. NCCoE part of the National Institute of Standards and Technology (NIST), the United States Department of Commerce is a collaborative center where industry organizations, government agencies, and academic institutions work together to tackle the world's most pressing Cybersecurity issues and a public-private collaboration to accelerate adoption extensive integrated cybersecurity tools and technology. The center forms a team with people from cybersecurity technology companies, other federal agencies and academics to address any problems.

If seen at the conditions that exist in European countries such as **Germany**, the strategy of cyber infrastructure protection is a shared responsibility and requires close collaboration between the government and the owner or operator of the infrastructure. The German government places the private sector as the main actor with an estimated 90%. Nevertheless, there are still institutions responsible for coordinating infrastructure protection policies at the government level. This is the Center for the Protection of Critical Infrastructure within the Federal Office for Civil Protection and Disaster Response (Federal Ministry of Interior). The agency is tasked with disseminating information and awareness of the protection of critical infrastructure, public-private partnerships, analysis and protection concepts, and protection measures, with a policy framework that is the baseline protection concept.

Then in Malaysia, in 2005 the Ministry of Finance and the Ministry of Science, Technology and Innovation established the National ICT Security and Emergency Response Center (Cybersecurity Malaysia) under the Malaysian Ministry of Communication and Multimedia. Once established, Cybersecurity Malaysia formed an official branch in the northern area of the Office at the Trade Center to support and support Cybersecurity. In addition, the Malaysian government also established a Laboratory that provides vulnerability assessments and ICTs for evaluating Cybersecurity. Malaysia also launched CyberSafe in Jakarta, as a Cybersecurity awareness program for all people and forms rather than cyber diplomacy. Cybersecurity Malaysia is led by 10 councils appointed under the approval of the Malaysian Minister of Domestic Trade and Consumer Affairs and several appointed by the Minister of Science, Technology and Innovation.

Of the several countries that have been outlined, in principle, when Indonesia wants to strengthen defense in the cyber field, of course, it must form an institution or agency that will become the leading sector to create integrated and integrated governance of institutions. The establishment of a national Cybersecurity center that has been practiced by other countries is to deal with threats and attacks in cyberspace that can threaten the country's sovereignty. The government can also collaborate with various parties to support the creation of optimal Cybersecurity and resilience, such as involving the private sector, academic institutions, and the government can do as an effort to strengthen its strategy to overcome threats and attacks in cyberspace. Finally, to optimize the performance of the institutions or bodies established to create Cybersecurity and resilience, there should be supervision in carrying out their duties as practiced in Australia.

3.4 Challenges and Obstacles in the Implementation of Cybersecurity and Resilience in Indonesia

In general, discussions on the Draft Bill on Cybersecurity and Resilience must be carried out by involving public participation. The Draft Bill should be able to provide an overview of Indonesia's cyber strategy, both globally and domestically. Besides, care must also be taken to avoid inconsistencies between inter-article regulations, unclear regulatory focus, to the extent of potential threats to civil Laliberties[19]. Bearing in mind, the main principles in making legislation must be done transparently and involve broad public participation. Furthermore, a national Cybersecurity strategy is urgently needed to develop and implement effective Cybersecurity governance, build independence of Cybersecurity technology, prevent and manage threats, incidents, cyberattacks, enhance the security culture in cyberspace, and optimize Cybersecurity resources.

The development and strengthening of Cybersecurity policies in Indonesia should be integrated with national strategies in building a national Cybersecurity ecosystem that has been prepared by the Government. The strategy includes legal remedies, technical efforts covering standards and operations, organizational and institutional structuring of Cybersecurity subscribers within the scope of national interests, capacity building, or capacity building of human resources in the field of cyber-security and increasing international cooperation[20]. Another challenge going

[19] ELSAM. (2019*). Position Paper RUU Keamanan dan Ketahanan Siber: Problem dalam Pengaturan dan Ancamannya Terhadap Kebebasan Sipil*,. Jakarta: ELSAM, p. 22

[20] Ibid

forward in developing Cybersecurity policies is the nature of multidimensional cyber threats making handling not only the responsibility of state institutions. A comprehensive approach is needed to realize strong and well-integrated national Cybersecurity and security institutional arrangements and arrangements. The implementation of cyber defense in Indonesia is still experiencing problems because it has not become a coordinated national initiative. This includes not yet optimal national awareness and national vigilance of the majority of the public against various information security challenges such as cyber threats, Cyberattacks, cybercrime, cyber terrorists, cyber propaganda, cyber warfare to spreading false news through social media that can threaten national interests and interfere with the sovereignty and integrity of the Unitary Republic of Indonesia[21].

In establishing the concept of a national Cybersecurity strategy policy, the first thing to consider is the type of cyber threat faced and how much influence the attack has had on the national security system. By knowing the category of cyber threats, it is expected to develop steps, strategies, and methods in building deterrence by utilizing the facilities and capabilities of national resources to support the creation of national security in the context of maintaining national sovereignty. Therefore, a strategic policy is needed in the form of a special law that can be used as a guideline or legal umbrella in implementing and supporting national defense in the field of security and cyber resilience as the main capital in planning national defense strategies and policies.

4. Conclusion

Cybersecurity and resilience has become one of the trends that are the focus of strengthening and protecting each country. The sovereignty and resilience of a country is not only judged by how much military or economic power it has, but also depends on the aspects of mastery, use, and empowerment of cyberspace. The current condition of the implementation of Cybersecurity and resilience in Indonesia is still scattered in various institutions or stakeholders, each of which has governance guidelines. Various existing laws and regulations, in fact are not able to accommodate and reach the problems that exist in cyberspace. Because of this, a special law is needed to regulates Cybersecurity and resilience and create an integrated management of Cybersecurity and resilience itself. Various countries have established national Cybersecurity centers to prevent cyber threats and attacks that can threaten the country's sovereignty. The many incidents of Cyberattacks that have occurred in several countries have also become one of the real urgencies to immediately build defense in the cyber field in Indonesia. The Indonesian government should enact the regulation of Cybersecurity and resilience in a spesific regulation. This arrangement is a response to prevent and ward off threats and Cyberattacks in the future in order to create protection against state sovereignty.

[21] Gultom, R. (2014). *Kajian Strategis Lemhannas RI tentang Badan Cyber Nasional (BCN), Debidjianstrat Lemhannas RI, Rekomendasi Gubernur Lemhannas RI kepada Presiden RI*. Jakarta: Lemhanas RI, p. 7

5. References

BOOKS:

Barril, R. T. (2003). *Information Technology and Management.* New York: Mc Graw Hill.

BPPT, P. T. (2007). *Kajian Konvergensi Teknologi Informasi dan Komunikasi.* Jakarta: Pusat Teknologi Informasi dan Komunikasi BPPT.

Brascomb, A. W. (1986). *Toward A Law of Global Communication Network.* New York: Lognman.

Clarke, R. a. (2010). *Cyber War: The Next Threat to National Security And What To Do About It. .* New York: Harper Collins.

Dorman Andrew, S. M. (2002). *The Changing Face of Military Power: Joint Warfare in an Expeditionary Era (Cormorant Security Studies Series).* London: Palgrave Macmillan.

ELSAM. (2019). *Position Paper RUU Keamanan dan Ketahanan Siber: Problem dalam Pengaturan dan Ancamannya Terhadap Kebebasan Sipil,.* Jakarta: ELSAM.

Gultom, R. (2014). *Kajian Strategis Lemhannas RI tentang Badan Cyber Nasional (BCN), Debidjianstrat Lemhannas RI, Rekomendasi Gubernur Lemhannas RI kepada Presiden RI.* Jakarta: Lemhanas RI.

Hamzah, A. (1990). *Aspek-aspek Pidana di Bidang Komputer.* Jakarta: Sinar Grafika.

ID-SIRTII. (2018). *Laporan Tahunan.* Jakarta: ID-SIRTII.

ID-SIRTII. (2018). *Indonesia Cybersecurity Monitoring Report 2018.* Jakarta: Desember.

Kementerian Pertahanan Indonesia. (2014). *Pedoman Pertahanan Siber.* Jakarta: Kementerian Pertahanan Indonesia.

James R. & Langevin, M. T. (2011). *Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency .* Washington DC: Center for Strategic and International Studies.

BSSN. (2018). *Indonesia Cybersecurity Monitoring Report.* Jakarta: BSSN.

BSSN. (2018). *Rencana Strategis Badan Siber dan Sandi Negara Tahun 2018-2019.* Jakarta: BSSN.

Smith, M. (2015). *Research Handbook on International Law and Cyberspace.* Massachusetts: Edwar Elgar Publishing Limited.

T Franklin D. Kramer et al. (2009). *Cyberpower and National Security .* Washington Dc: National Defense University.

JOURNALS:

Gultom, R. A. (2017). Membangun Kemampuan Siber dan Persandian Nasional guna Mengantisipasi Tantangan Keamanan Siber di Era Globalisasi Informasi dalam Rangka Melindungi Keutuhan dan Kedaulatan NKRI,. *Jurnal Kajian Lemhanas*, 28.

Soepandji, K.W & Farid, M. (2018). Konsep Bela Negara dalam Perspektif Ketahanan Nasional,. *Jurnal Hukum dan Pembangunan*, 48(3), 436-456

Prasetyono, E. (2008). Strategi Pertahanan Indonesia di Masa Depan. *Jurnal Analisis CSIS.* 37(3), 347—361.

Sumari, A.D.W. & Setyawan, D.P. (2016). Diplomasi Pertahanan Indonesia dalam Pencapaian Cybersecurity melalui Asean Regional on Cybersecurity Initiatives. *Jurnal Penelitian Politik*, 13(1), 1-20.

THESIS AND DISSERTATION :

Kustiyawan, I. (2012). *Kajian Strategi Keamanan Cyber Nasional: Dalam Rangka Meningkatkan Ketahanan Nasional di Bidang Keamanan Cyber.* Tesis Universitas Pertahanan Indonesia.

Ramadhan, M. F. (2019). *Kepentingan Singapura pada Keamanan Siber di Asia Tenggara dalam Singapore International Cyber Week*. Padjajaran Journal of International Relations .

Rhynaldie, K. B. (2019). *Regulasi Penanganan Kejahatan Siber di Lingkungan TNI Angkatan Darat*. Tesis Universitas Terbuka Bogor.

PAPERS

Gultom, R. (2015). Cyberspace as Global Domain Materials of Cybersecurity For Information Leaders Course, The National Defense University (NDU). Washington Dc.

ONLINE

Gautama, H. (2020). *Cybersecurity*. Retrieved from: http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf , Accessed on April 10 2020.

Cybersecurity. (2020). www.asd.gov.au: https://www.asd.gov.au/cyber (accessed on April 18 2020

Informatika, K. K. (2020). http://aptika.kominfo.go.id/index.php/artikel/86-kebijakankeamanan-danpertahanan-siber-2 , Accessed on April 19 2020

Pertahanan, K. (2020). https://www.kemhan.go.id/bainstranas/2019/07/22/pushansiber-ikut-serta-dalam-fgd-kedaulatan-siber-dan-data.html, Accessed on April 2 2020.

LEGAL ADAGE

LEX REJICT SUPERFLUA, PUGNANTIA, INCONGRUA

The Law Rejects Contradictory and Improper Things