Indonesian Cyber Law Indonesian Cyber Law Formulation in The Development of National Laws in 4.0 Era

Rama Halim Nur Azmi
Faculty of Law, Brawijaya University
Jl. M.T. Haryono 169, Ketawanggede, Lowokwaru, Malang City, East Java 65145

Article Info: Submitted April 1, 2020 Accepted April 26, 2020
Published May 9, 2020

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

Abstracts :
The digital age has made the loss of boundaries for interaction and communication which then creates a new world of cyberspace. The cyberspace entity on the one hand provides advantages and on the other hand also causes losses if there is no protection in the cyberspace. Protection of cyberspace in Indonesia is still far from good and tends to be bad. Even President Susilo Bambang Yudhoyono has been a victim of the weak protection of the cyberspace. These weaknesses are the implications of the existence of norms that are legal norms which are the basis of the implementation of cyberspace protection in Indonesia. In this paper , we will discuss about the problems of cyberspace in Indonesia and how legal norms should be present as a means of social control and engineering. Especially, the cyberspace in order to realize order and security in the cyberspace. The method used in this study is the normative juridical method with the legislation approach and case approach.

Keyword: *Digital era; cyberspace; void norms; legal norms*

Abstrak :
Era digital telah membuat hilangnya batas wilayah untuk berinteraksi dan berkomunikasi yang kemudian menciptakan dunia baru yakni ruang siber. Entitas ruang siber tersebut di satu sisi memberikan keuntungan dan di sisi lain juga menimbulkan kerugian apabila tidak adanya perlindungan di ruang siber. Perlindungan ruang siber di Indonesia masih jauh dari kata baik dan cenderung buruk. Bahkan Presiden Susilo Bambang Yudhoyono pernah menjadi korban dari lemahnya perlindungan ruang siber tersebut. kelemahan tersebut merupakan implikasi dari adanya kekosongan norma yakni norma hukum yang menjadi landasan penyelenggaraan perlindungan ruang siber di Indonesia. Dalam tulisan ini akan dibahas mengenai problematika yang terjadi dalam ruang siber di Indonesia dan bagaimana seharusnya norma hukum hadir sebagai alat kontrol dan rekayasa sosial terutama dalam ruang siber tersebut guna mewujudkan ketertiban dan keamanan dalam ruang siber tersebut. Metode yang digunakan dalam penelitian ini yakni metode yuridis normatif dengan pendekatan peraturan perundang-undangan dan pendekatan kasus.

Kata Kunci : *Era digital; ruang siber; kekosongan norma; norma hukum;*

Citation :
Azmi, R.H.N. (2020). Indonesian Cyber Law Formulation in the Development of National Laws in 4.0 Era. Lex Scientia Law Review 4(1), 49-62. doi: https://doi.org/10.15294/lesrev.v4i1.38109

1. Introduction

Globalization and current technological developments have changed the social structure of Indonesian society. In this current era, the existence of electronic devices seems to have become an inseparable part of people's daily lives. Today everything is done with the help of electronic devices so that it is known as the 4.0 era. This certainly shows that there are developments in social life where these developments indirectly also participate in changing social institutions and norms that grow and develop in society, one of which is legal norms.

Legal norms are one of the institutions that regulate social life to create an organized life. This is a form of legal function as social control (law as social control) in social life. However, between the dynamics of social development and law does not go hand in hand. The social development of society takes place very quickly, while the development of law takes place slowly. So that comes the expression "the law limped along with the incident" (*het recht hinkt achter de feiten aan*). The phrase shows that the existence of law always lags behind the social development of society.

However, one of the German legal experts, Frederich Carl Von Savigny, said that law is actually a living entity (*es ist und wird mit dem volke*) and develops along with the development of society, on the basis of its own moral authority. In this case, the law must continue to function or mean for the interest and order community order (Rosana, 2013). In addition, there is one perspective on the correlation between law and community development known as responsive legal perspectives. This was revealed by Phillipe Nonet and Phillipe Selznick. In their argument, Nonet and Selznick stated that "only responsive law promises a stable and lasting institutional order".In the type of responsive law by nonet. She rejects final legal autonomy and cannot be contested. The Responsive legal theory is a legal theory that contains a critical view. This theory states that law is a means to an end. Responsiveness is defined as serving the needs and social interests experienced also discovered by the people. Responsiveness implies a commitment to "law in the perspective of the consumer".[1]

In the 1945 Constitution, Indonesia has been affirmed as a constitutional state as regulated in Article 1 paragraph (3). As a rule of law, it has become the main characteristic that all actions of the State go through, based on and under the law.[2] In this case, it becomes an obligation in all aspects of national and state life to always be based on applicable law. One of them is national defense and security aspects. Defense and state efforts are are listed in the fourth paragraph Preambule of the 1945 Constitution, which states that "to protect all Indonesians and all the blood of Indonesia and to improve the welfare of society, develop the life of the nation, and participate in carrying out the world order based on independence and eternal peace".Then, the purpose of the country is manifested in Chapter XII on National Defense and Security in Article 30 of the 1945 Constitution of the Republic of Indonesia.

The Montenvideo Convention 1933 explains about the essential elements of state. One of the elements is state has a certain area. The area is only defined physically, such as: land, sea, and water. However, in the current technological era, the region is not only defined physically but also non-physically or well known as cyberspace.

Cyberspace is a virtual place, in which communication through internet media takes place.[3] The term cyberspace was first introduced by William Gibson in 1980 in his fictional works entitled Neuromancer.[4] Because the term comes from fiction, what William Gibson said was only a description of how cyberspace is in the world of ideas. Currently, many experts are trying to provide definitions related to cyberspace, for example, Abdul Wahid and Mohammad Labib. They define cyberspace as a new reality

[1] Nonet, P., & Selznick, P. (2001). *Law and Society Transtition: Toward Responsive Law. Dalam S. Arinanto, Politik Hukum 2.* Jakarta: Pascasarjana Fakultas Hukum Universitas Indonesia, p.11
[2] Simorangkir, J. (1983). *Hukum dan Konstitusi Indonesia.* Jakarta: Gunung Agung, p. 34
[3] Vivian, J. (2008). *Teori Komunikasi Massa.* Jakarta: Kencana, p.23
[4] Buick, J., & Jevtic, J. (1997). *Mengenal Cyberspace For Beginners.* Bandung: Mizan p. 44

or nature formed by the internet medium which creates new communities as citizens (netizens).[5] The existence of a new reality that was previously only real is now added to the virtual nature. This virtual reality is often associated with the internet and cyberspace.[6]

In this current era, encouraging the potential of war between countries by using traditional to conventional methods of war. As a result, state power is not only limited to the strength of weapons, but also in terms of culture, economy, politics, and technology. The form of war has also shifted. War was previously identified as heavy class warfare. Nowdays the war is moving in a new direction called the war in cyberspace using internet media.[7] The threat of attacks in cyber space is not only performed by actors other State *(state actors)* but also actors non-state *(non-state actors),* for example individual hackers, groups hacker, non-governmental organization (NGO), terrorism, organized crime groups, and the private sector (such as internet companies and carries, security companies) that can threaten the defense and sovereignty of the State.[8]

Threats in the cyberspace carried out by those actors. They are carried out either intentionally with various existing motives for example to obtain financial, military and political advantages, or inadvertently such as showing existence or just trying. Cyberspace has become a threat to the State due to its scope which can be used to steal information, spread destructive ideas, or attack on information systems in various fields, such as banking data, military networks, and even the national defense system.[9]

The existence of a paradigm shift regarding the concept of national defense and security which has been related to the region physically created a current issue for discussion. This is mainly about the juridical aspects of the concept of national defense and security in the cyberspace. In this paper, we will discuss about the problem of cyberspace in Indonesia and how legal norms should be present as a means of social control and engineering. Especially, in order to realize security of cyberspace.

Research Problems

Based on the background that the writer described before, the formulation of the problem that can be drawn to determine the focal point in the next discussion is as follows:

1. What is the problem with cyberspace in Indonesia?
2. What is the proper construction of legal norms to protect the cyberspace?

The purpose of writing

1. Knowing how the problems that occur in the Indonesian cyberspace.
2. Knowing how the construction of legal norms is right to protect cyberspace in Indonesia.

State of Act

[5] Wahid, A., & Labib, M. (2005) *Kejahatan Mayantara (Cyber Crime).* Jakarta: Refika Aitama p. 12

[6] Ibid.

[7] Rahmawati, I. (2017). Analisis Manajemen Risiko Ancaman Kejahatan Siber (Cyber Crime) dalam Peningkatan Cyber Defence. *Jurnal Pertahanan & Bela Negara.* 7(2), p. 52

[8] Pearlman, W., & Cunningham, K. (2012). Non-State Actors, Fragmentation, and Conflict Processes. *Journal of Conflict Resolution*, p. 4

[9] Smith, M. (2015). *Research Handbook on International Law and Cyberspace.* Massachusetts :Edwar Elgar Publishing Limited, p. 18

Research on cyberspace has been carried out by many academics, practitioners, and experts both national and international writers. However, previous studies only focused on threats in cyberspace, the establishment of cybersecurity task forces, or the study of cyberspace. In this study, The Author carried out a theoretical study accompanied by case studies which tried to create a structured, systematic and massive Indonesian cyberspace protection formulation starting from protection in terms of juridical (substance) to related parties as implementing the protection of the cyberspace (structure).

2. Research Methods

The type of research in this article is normative juridical or also called doctrinal law research. [10]The researcher examines primary legal material,[11] and then proceed with research on secondary legal materials to answer the problems that are the focus of research that conceptualizes the concept of research. The law as a rule or norm which is a benchmark for human behavior that is deemed appropriate. The writing approach method used in this study is the statute approach by analyzing the statutory regulations. [12] Case approach by examining and understanding cases related to problems that occur due to the absence of norms that govern the implementation of national defense and security efforts in cyberspace.[13]

3. Result and Discussion

3.1 The Problem of Cyber Space in Indonesia

In this digital age, interaction and communication are carried out by everyone without recognizing the existence of borders (borderless). This certainly shows the existence of an easy access, speed and connectivity from the internet into something that is widely used by people in various countries aspects of life with easy distribution of information. Along with the use of a computer system network that uses telecommunications system infrastructure makes people as users as if discovering a new world. This concept is often referred to as cyberspace.[14]

Indonesia is a country with the largest internet users in the world. This is proven by Statista data which shows Indonesia ranked fifth with 143.26 million internet users as of March 2019. This figure has a slight difference of 5.8 million with Brazil which has 149.06 million internet users. The top rankings were obtained by China with 829 million internet users. Second place is India. This country has a considerable difference with China up to 269 million with 560 million internet users.United States (US) followed by internet usersas many as 292.89 million.[15]

[10] B., S. (n.d). *Karakter Penelitian Hukum Normatif dan Sosiologis* . Yogyakarta: Puskumbangsi LEPPA UGM.

[11] Soemitro, R. H. (1998). *Metodologi Penelitian Hukum dan Jurimetri.* Jakarta: Ghalia, Jakarta, p. 34

[12] Widnjoesoebroto,S. (2002). Hukum, Paradigma, Metode, dan Dinamika Masalahnya, Jakarta: Elsam-Huma, p. 9

[13] Marzuki, P. M. (2005). *Penelitian Hukum.* Jakarta: Kencana, p. 66

[14] Sanusi, M. A. (2005). *Hukum Teknologi dan Informasi.* Bandung: Tim Kemas Buku, p. 29

[15] Jayani, D. H. Berapa Pengguna Internet di Indonesia? Retrieved from: https://databoks.katadata.co.id/datapublish/2019/09/09/berapa-pengguna internet-di-indonesia, Accessed on February,17 2020.

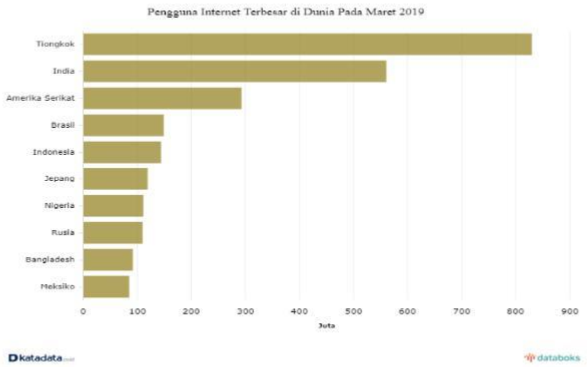

Figure 1. 10 of the World's Largest Internet Users
(Source: Katadata Databooks)

In addition, Statistics data shows that Indonesian internet users in 2018 were 95.2 million. This is grown by 13.3% from 2017 which was 84 million users. In the 2018-2023 periods, Indonesian internet users in Indonesia will increase with an average growth of 10.2%. In 2019, the number of internet users in Indonesia is projected to grow 12.6% compared to 2018, which are 107.2 million users. In 2023, the number of internet users in Indonesia is projected to reach 150 million users. The Statistics also mentioned that popular online activities in Indonesia are social media and cellular messaging.[16]

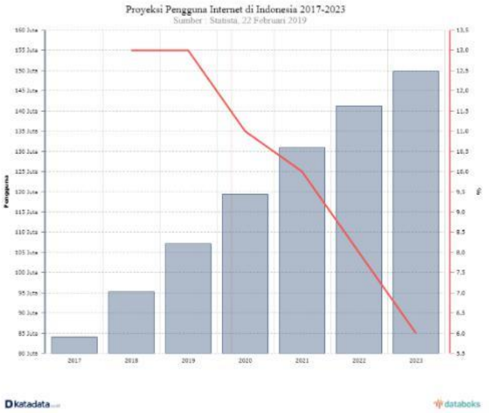

Figure 2. Projection of Internet Users in Indonesia 2017 - 2023
(Source: Katadata Databooks)

In the industrial revolution 4.0 eras, which prioritizes digitalization in all sectors of the economy needs serious attention regarding the cyber threat. Indonesia is a country in Southeast Asia with the most rapid digital economic growth in the last 5 (five) years. As data from Google, Temasek, and Bain Company states that in 2019, the digital economy in Indonesia has reached US $ 40 billion or grew five times compared to 2015 which only reached US $ 8 billion alone.[17]

[16] Ibid

[17] Putri, C. A. *Terungkap! Ekonomi Digital RI Tumbuh Paling Pesat di ASEAN*. Retrieved form: https://www.cnbcindonesia.com/tech/20191007160823-37-105004/terungkap-ekonomi-digital-ri-tumbuh-paling-pesat-di-asean, Accessed on March 9 2020.

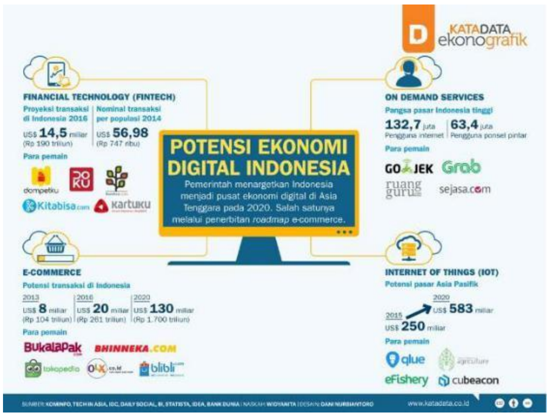
KATADATA ekonografik
FINANCIAL TECHNOLOGY (FINTECH)
Proyeksi transaksi di Indonesia 2016
US$ 14,5 miliar (Rp 190 triliun)
Nominal transaksi per populasi 2014
US$ 56,98 (Rp 747 ribu)
Para pemain
dompetku
DOKU
Kitabisa.com
kartuku
POTENSI EKONOMI DIGITAL INDONESIA
Pemerintah menargetkan Indonesia menjadi pusat ekonomi digital di Asia Tenggara pada 2020. Salah satunya melalui penerbitan roadmap e-commerce.
ON DEMAND SERVICES
Pangsa pasar Indonesia tinggi
132,7 juta Pengguna internet
63,4 juta Pengguna ponsel pintar
Para pemain
GO-JEK
Grab
ruang guru
sejasa.com
E-COMMERCE
Potensi transaksi di Indonesia
2013 US$ 8 miliar (Rp 104 triliun)
2016 US$ 20 miliar (Rp 261 triliun)
2020 US$ 130 miliar (Rp 1.700 triliun)
Para pemain
BukaLapak
BHINNEKA.COM
tokopedia
OLX.co.id
blibli.com
INTERNET OF THINGS (IOT)
Potensi pasar Asia Pasifik
2015 US$ 250 miliar
2020 US$ 583 miliar
Para pemain
qlue
agriculture
eFishery
cubeacon
SUMBER: KOMINFO, TECH IN ASIA, IDC, DAILY SOCIAL, BI, STATISTA, IDEA, BANK DUNIA | NASKAH: WIDYANITA | DESAIN: DANI NURBIANTORO
www.katadata.co.id

Figure 3. The Potential of Indonesia's Digital Economy
(Source: Econographic Katadata)

Indonesia currently has a lot of start-ups that have unicorn status or decacorns such as Gojek, Bukalapak, Tokopedia, Blibli.com, and others. This is certainly concrete evidence that the stretch of t digital economy in Indonesia cannot be underestimated. The rapid development of digital economy can certainly contribute to the improvement of the economy and national income which leads to the improvement of people's welfare. The government is currently declaring Indonesia as the largest digital economy in 2020. This is targeted to be the largest in Southeast Asia. One of the foundations of national development in this declaration is the digital sector. The government is targeting e-commerce transactions to reach US $ 130 billion and creating 1000 technopreneur with a business value of US $ 10 billion in 2020.[18]

In an effort to create a good digital economic climate, of course a protection mechanism is needed for data traffic in the cyber world. Based on various events in the past few years, Indonesia is a weak cyber-security country. This can be seen from the rise of various cases of hacking, one of which is hacking of a bank customer debit card data because hackers try to infiltrate the bank customer card security system that occurred in mid-May 2014 makes a note of how bad cyber-security in Indonesia.[19]

Indonesia also has long been involved in the several cyber warfare with other countries.Around 1998 Indonesia was involved in cyberwarfare with China and Taiwan relating to social and political conflicts that led to racial conflict. Then in 1999, another war in the cyber world took place again between Indonesia and Portugal relating to the liberation of East Timor as one of the provinces in Indonesia which was finally released and became its own country. In recent years, there have been frequent attacks in cyberspace between Indonesian and Malaysian hackers. This action usually starts when there is political conflict or competition between the two countries. Although it did not involve the governments of the two countries, the actions of these

[18] Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informasi Republik Indonesia. (n.d). *Study Ekonomi Digital di Indonesia sebagai Pendorong Utama Pembentukan Industri Digital Masa Depan.* Jakarta: Badan Penelitian dan Pengembangan SDM Kemenkominfo RI,
[19] Ardiyanti, H. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica*l, 5(1) , p. 99

hackers attacked the cyber infrastructure of the Malaysian and Indonesian governments.[20]

In 2013, based on leaked documents from Edward Snowden, a former member of the United States National Security Agency (NSA), Indonesia became a victim of wiretapping by Australian intelligence agencies. In the document leaked Snowden contains a list of tapping targets that show the name of Indonesian President Susilo Bambang Yudhoyono, his wife, and some of the closest people in the president's environment.[21] The wiretapping of Indonesia is carried out by the United States NSA the same as the Australian Directorate of Defense Codes (DSD). Reason Australia helps the United States to conduct wiretapping is to advance its own national interests and as a contribution to the alliance with the United States.[22] The case is one of the cases which show that the weakness of Indonesia's cyber-security threatened the Indonesian President at that time.

Some of the cyber crime attacks are only a small part that occurred in Indonesia, there are many more cyber attacks that occur in Indonesia with various patterns of mode and purpose. For example, the big cyber attack by Ransomware Wannacry. This malware was detected early entering the territory of Indonesia since it attacked the cyber system owned by Harapan Kita Hospital and Dharmais, hundreds of servers and computers used for hospital operations were affected, so activities in the hospital were disrupted. After attacking the hospital, Wannacry's Ransomware quickly spread on servers and computers in Indonesia, until the Ministry of Communication and Information issued a press release to inform information of this malware by issuing press releases press release no. 55/HM/KOMINFO/05/2017 concerning the appeal and preventive measures for the *Ransomware Wannacry malware*.[23]

Based on the Honeynet Project's Report 2018, the total number of cyberattacks that attacked Indonesia on the 21 sensors that have been installed 12,895,554 attacks, with a total malware of 513,863 attacks. There are three sources of the highest attacks coming from Russia (2,597,256 attacks), China (1,871,363 attacks), and the United States (1,428,440 attacks). The highest target ports affected by the attack are on theport SMBD (2,071,320 attacks), SipSession (1,298,691 attacks), and SipCall (1,187,560 attacks). The highest number of attacks based on the type of malware is Win32/Conficker.worm.167765 (429,208 attacks). In 2018, IP CNC that received the highest attacks were 176.15.11.122 (392,721 attacks), 176.15.11.56 (303,496 attacks), and 128,199,115,119 (300,063 attacks).

An ironic fact is conveyed by Akamai as a well-known internet monitoring company in which Indonesia is the country that has the highest target of cyber attacks. Indonesia is at the first level as the country with the highest threat of cyber attacks in the world which was previously occupied by China. Of the 175 countries investigated, Indonesia contributed as much as 38 percent of the total target of hacking traffic on

[20] Manthovani, R. (2006). *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia*. Jakarta: Malibu, p.45

[21] Tanter, R. (2014). Indonesia, Australia and Edward Snowden: Ambiguous and Shifting Asymmetries of Power. *The Asia Pasific Journal*, 12(3), p. 5

[22] Lisbet. (2013). *Sikap Indonesia Terhadap Isu Penyadapan Amerika Serikat dan Australia.* Pusat Pengkajian. Jakarta: Pengolahan Data dan Informasi DPR RI, p. 80

[23] Kementerian Komunikasi dan Informasi Republik Indonesia. (2017). *Himbauan Agar Segera Melakukan Tindakan Pencegahan terhadap Ancaman Malware Khususnya Ransomware Jenis Wannacry. Kementerian.* Jakarta: Komunikasi dan Informasi Republik Indonesia, p. 50

the internet. This number increases with the increase of internet speed in Indonesia. According to David Belson of Akamai Research, internet speed has no connection with the large potential of internet crime that threatens Indonesia. Hacking is more due to the weakness of the internet and computer security system in Indonesia.

Losses caused by crime with using the cyber world in Indonesia according to CIA data have reached 1.20% of the level of losses due to cybercrime that occurred in the world as shown in the following table:

Global	Indonesia	
GDP:	USD 71,620 bn	USD 895 bn
Percent of global GDP:	1,20 %	
Cost of:		
Genuine cyber crime:	USD 3,457 m	USD 43 m
Transitional Cyber crime:	USD 46,600 m	USD 582 m
Cyber criminal infrastructure:	USD 24,840 m	USD 310 m
Traditional crimes becoming cyber	USD 150,200 m	USD 2,748 m

Table 1. Estimated Losses Due to Cyber Crime in the World and Indonesia *(Source:* (DAKA Advisory, 2014)

From the estimated table of losses due to cyber crime that compares the estimated losses caused by cyber crime in Indonesia at USD 895 billion, which means that it reaches 1.20% of the total estimated losses due to cyber crime globally reaching USD 71.620 billion.[24] Losses due to cyber crime cannot be underestimated because in addition to showing the vulnerability of Indonesia's cyber security the data also shows potential obstacles in the development of the digital economy in Indonesia. This condition must receive serious attention from the government, especially with regard to the government's strategic plan to develop Indonesia's digital economy.

3.2 Problem and Resolution Factors

In the context of the rule of law, especially those adopting civil law like Indonesia, the existence of statutory regulation as the legal basis for organizing all actions is an inevitable necessity. Until now, Indonesia does not have any legislation related to cybersecurity and security.Previously, the Indonesian House of Representatives (DPR RI) had the chance to ratify the Draft Cyber Security and Resiliency Act. However, this was not carried out due to rumors circulating that there were controversial articles in it and there was a formal defect in the formation of the draft law.

With the concept of the rule of law adopted by Indonesia, it becomes a necessity that as a basis for maintaining the sovereignty of the state in the digital era at this time it is needed a statutory regulation governing it. As a rule of law, all aspects of life in

[24] Ibid.,102

the social, national, and state fields including the government must be based on laws that are under the national legal system. Because the principle of the state of law adopted by Indonesia is a modern state of law, well known as the Pancasila State of Law, the statutory provisions of the invitation-only give shape to the values and norms that live in society and can barely change the function of the state in the field of regulation. But the invitation regulation is one of the effective methods and instruments present to give and direct the lives of the people towards their desired goals. In a modern state of law, legislation expected to be able to "go ahead" lead and guide the development and change of society.[25]

One expert on Indonesian law and regulation, Maria Farida Indrati, stated that in a country based on modern law, the main purpose of forming laws is no longer creating codifications for norms and values that have settled in society will but the main purpose of forming the law is creating modifications or changes in people's lives.[26] Yuliandri stated that the "legal policy" as outlined in the law, became a means of social engineering, which contained the policies to be achieved by the government, to direct the community to accept new values.[27] Whereas Hattu states that in a modern state of law require the formation of laws and regulations that serve as an instrument to give regulate, limit, as well as oversee the implementation of the duties and authorities of the government and guarantee the rights of the people.[28]

In his book, Code: Version 2.0 (2006), which is a revised edition of the previous book, Code and Other Laws of Cyberspace (2000), Lawrence Lessig mentions the matter of regulability in cyberspace. Regulability is the ability of governments to regulate behavior to the proper domain. In the context of the internet, regulability means the ability of governments to regulate the behavior of citizens on the internet.[29] So, it is clear that a regulation on cyber security and security is needed supported by the protection of personal data as a legal basis in the effort to create a state sovereignty in the digital age and efforts to create a digital industry climate that is free from cyber threats.

Although, there are already laws and regulations that govern them but an implementation is needed to carry out the mandate of the law. The power of cyber defense must be prepared optimally. This was done to establish a cyber defense system to protect cyberspace from all threats both from Indonesia itself and from outside Indonesia. Various cyber attacks that occur in Indonesia ranging from hackers, cyber warfare, wiretapping of the President of the Republic of Indonesia, the spread of malware to infrastructure, and other cyber attacks shows that the condition of Indonesia's cyber defense is of high concern. To deal with this, a comprehensive assessment and solutions from all lines are needed so as to be able to create a strong cyber defense and security system. Cybersecurity is a collection of tools, policies, security concepts, security protections, guidelines, risk management approaches, actions, training, best practices, guarantees and technology that can be used to protect cyberspace and the organization and user assets. Organization and assets of users in

[25] Tim Pengajar Teori Perundang-Undangan Fakultas Hukum Universitas Indonesia. (2009). *Teori Perundang-Undangan*. Jakarta: Badan Pembinaan Hukum Nasional, p. 34

[26] Indrati, M. F. (2002). *Ilmu Perundang-Undangan: Jenis, Fungsi, dan Materi Muatan.* Yogyakarta: Kanisius, p. 76

[27] Yuliandri. (2011*). Asas-Asas Pembentukan Peraturan Perundang-Undangan yang Baik: Gagasan Pembentukan Undang-Undang Berkelanjutan*. Jakarta: Rajawali Press, p. 46

[28] Hattu, H. (2011). Tahapan Undang-Undang Responsif. *Jurnal Mimbar Hukum*, 23(2), p. 406

[29] Lessig, L. (2006). *Code: Version 2.0*. New York: Basic Books, p. 17

cyber-security, including devices connected to computing, personnel, infrastructure, applications, services, telecommunications systems and the totality of information transmitted and/or stored in a virtual environment. Cyber-security is an effort to ensure the achievement and maintenance of the security characteristics of the organization and user assets against relevant security risks in the cyber environment. General security objectives consist of availability; Integrity includes authenticity and the possibility of efforts to reduce the occurrence of rejection and finally confidentiality.

Cybersecurity policies specifically in Indonesia have been initiated since 2007 with the issuance of the Minister of Communications and Regulation Informatics No.26/PER/M.Kominfo/5/2007 concerning Safeguarding the Utilization of Internet Protocol-Based Telecommunications Networks which was then revised by Minister of Communication and Information Regulation No.16/PER/M.KOMINFO/10/2010 which was later renewed with regulations Minister of Communication and Information No.29/PER/ M.KOMINFO/12/2010.[30] However, the Permenkominfo is certainly not enough to be the basis for the protection of cybersecurity and resilience in Indonesia. In this case, a product of law is needed that specifically regulates the mechanism of protection of cybersecurity and resilience.

In the process of its formation, the DPR and the government must provide opportunities for public participation. This is needed as a form of transparency and community participation in the process of forming the law. So that, Later the law can be accepted for existence and validity in the community. In addition, in the formation of this law on cybersecurity and resilience, it will also be necessary to synchronize and harmonize both vertically and horizontally so that there is no norm conflict between one law and another. In the law on cybersecurity and resilience, it must also be confirmed which institutions are authorized to participate in the protection of cybersecurity and resilience. Then, in the implementation also how the division of authority so that the creation of a legal certainty related to the authority of each institution. This is also to avoid overlapping authority between institutions with one another.

The law that has been made subsequently becomes the basis for relevant parties to implement cyberspace protection in Indonesia. In the effort to protect all parties such as the Ministry of Defense (Kemenhan), the Indonesian National Army (TNI), the Indonesian National Police (Polri), the National Siber and Cipher Agency (BSSN), and the National Intelligence Agency (BIN), as well as other parties must synergy and collaborate with each other. This is necessary so that no conflict of authority between these institutions will create a gap in the cyber protection effort. Even if it is deemed necessary the parties can form a task force that specifically performs the duties and functions in order to protect and maintain cyberspace in Indonesia.

4. Conclusion

Based on the problems that the authors have described, it can be concluded that in the current era of technological advancements not only discuss a real space but also space in cyberspace or cyberspace. In a virtual space, it certainly cannot be separated from things that can threaten a country's sovereignty and even damage the digital economic climate in a country. Based on available data, it can be seen that the growth

[30] Ibid.,108

and development of the digital industry in Indonesia is developing very rapidly. The current government also moves businesses to expand into the digital sector.

In this case, Government as the highest authority in a country is obliged to protect everything that can damage the climate digital economy in Indonesia. This is in addition to protection towards state sovereignty as well as efforts to provide a sense of security and protection for the digital industry in Indonesia. In order to realize this, a structured, systematic and massive construction is needed, accompanied by a synergy of related parties as executors in the field.

In creating a construction of such protection, it must start from the existence of a regulation that explicitly regulates the protection of the cyber world. This is certainly as a step to create a legal certainty so that there is a solid foundation. Furthermore, the regulation certainly needs to be executed by related parties such as the Ministry of Defense, TNI, Polri, and BSSN as institutions that have the qualifications in protecting cyberspace. However, So far the problem has been that there is still a sectoral framework that causes a lack of harmony and synergy between the parties. In addition to these parties, community support is also needed to participate in maintaining and securing cyberspace. With a structured, systematic, and massive cyber protection construction, it is expected to be a facility to protect the cyberspace in Indonesia.

5. Acknowledgments

First of all, the writer wants to express gratitude to God Almighty because for his blessings, mercy, and guidance this writing can be completed properly. The author also wants to thank the family who always supported both materially and immaterially. In addition, the authors also thank the Faculty of Law, Universitas Brawijaya as a place for writers to learn and gain knowledge so that the author is able to conduct scientific studies that can be set forth in this paper.

6. References

Books

B., S. (n,d) . *Karakter Penelitian Hukum Normatif dan Sosiologis.* Yogyakarta: Puskumbangsi LEPPA UGM.

Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informasi Republik Indonesia. (n,d). *Study Ekonomi Digital di Indonesia sebagai Pendorong Utama Pembentukan Industri Digital Masa Depan.* Jakarta: Badan Penelitian dan Pengembangan SDM Kemenkominfo RI.

Buick, J., & Jevtic, J. (1997). *Mengenal Cyberspace For Beginners.* Bandung: Mizan.

DAKA Advisory. (2014). *Meeting the cyber-security challenge in Indonesia An Analysis of Threats and Responses.* DAKA Advisory.

Ibrahim, J. (2007). *Teori dan Metodologi Penelitian Hukum Normatif.* Malang: Banyumedia.

Indrati, M. F. (2002). *Ilmu Perundang-Undangan: Jenis, Fungsi, dan Materi Muatan.* Yogyakarta: Kanisius.

Kementerian Komunikasi dan Informasi Republik Indonesia. (2017). *Himbauan Agar Segera Melakukan Tindakan Pencegahan terhadap Ancaman Malware Khususnya Ransomware Jenis Wannacry.* Jakarta: Kementerian Komunikasi dan Informasi Republik Indonesia.

Lessig, L. (2006). *Code: Version 2.0.* New York: Basic Books.

Lisbet. (2013). *Sikap Indonesia Terhadap Isu Penyadapan Amerika Serikat dan Australia.*

Jakarta: Pusat Pengkajian, Pengolahan Data dan Informasi DPR RI.

Manthovani, R. (2006). *Problematika dan Solusi Penanganan Kejahatan Cyber di Indonesia.* Jakarta: Malibu.

Manthovani, R. (2006). *Problematika dan Solusi Penanganan Kejahatan Siber di Indonesia.* Jakarta: Malibu.

Marzuki, P. M. (2007). *Penelitian Hukum.* Jakarta: Kencana.

Nonet, P., & Selznick, P. (2001). Law and Society Transtition: Toward Responsive Law. Dalam S. Arinanto, *Politik Hukum 2.* Jakarta: Pascasarjana Fakultas Hukum Universitas Indonesia.

Sanusi, M. A. (2005). *Hukum Teknologi dan Informasi.* Bandung: Tim Kemas Buku.

Simorangkir, J. (1983). *Hukum dan Konstitusi Indonesia.* Jakarta: Gunung Agung.

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

Edwar Elgar Publishing Limited.

Soemitro, R. H. (1988). *Metodologi Penelitian Hukum dan Jurimetri.* Jakarta: Ghalia.

Tim Pengajar Teori Perundang-Undangan Fakultas Hukum Universitas Indonesia.

(2009). *Teori Perundang-Undangan.* Jakarta: Badan Pembinaan Hukum Nasional.

Vivian, J. (2008). *Teori Komunikasi Massa.* Jakarta: Kencana.

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime).* Jakarta: Refika Aitama.

Widnjoesoebroto, S. (2002). *Hukum, Paradigma, Metode,dan Dinamika Masalahnya.*

Jakarta: ELSAM-HUMA.

Yuliandri. (2011). *Asas-Asas Pembentukan Peraturan Perundang-Undangan yang Baik: Gagasan Pembentukan Undang-Undang Berkelanjutan.* Jakarta: Rajawali Press.

Journals

Ardiyanti, H. (2014). Cyber-Security dan Tantangan Pengembangannya di Indonesia.

*Jurnal Politica*l, 5(1), 95-110.

Hattu, H. (2011). Tahapan Undang-Undang Responsif. *Jurnal Mimbar Hukum*, 23(2), 406-419.

Pearlman, W., & Cunningham, K. (2012). Non-State Actors, Fragmentation, and Conflict Processes. *Journal of Conflict Resolution*, 13(2), 352-351.

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

Rosana, E. (2013). Hukum dan Perkembangan Masyarakat. *Jurnal TAPIs*, 9(1), 100-118.

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defence sebagai Upaya Mempertahankan Kedaulatan Negara. *Jurnal Perspektif, XXI*, 21(3), 168-187

Tanter, R. (2014). Indonesia, Australia and Edward Snowden: Ambiguous and Shifting Asymmetries of Power. *The Asia Pasific Journal*, 12(3), 1-14

Online

Biro Hukum dan Humas Badan Siber dan Sandi Nasional. (2019). *Mengenali Serangan Siber Global dan Nasional Melalui Laporan Tahunan Honeynet Project*

BSSN-IHP Tahun 2018. Retrieved From Badan Siber dan Sandi Nasional: https://bssn.go.id/mengenali-serangan-siber-global-dan-nasional-melalui-laporan-tahunan-honeynet-project-bssn-ihp-tahun-2018/ , diakses pada 3 Februari

Jayani, D. H. (2019). *Berapa Pengguna Internet di Indonesia?* Diambil kembali dari Databooks Katadata.co.id: https://databoks.katadata.co.id/datapublish/2019/09/09/berapa-pengguna-internet-di-indonesia , diakses pada 17 Februari 2020

Putri, C. A. (2019). *Terungkap! Ekonomi Digital RI Tumbuh Paling Pesat di ASEAN*. Diambil kembali dari CNBC Indonesia: https://www.cnbcindonesia.com/tech/20191007160823-37-105004/terungkap-ekonomi-digital-ri-tumbuh-paling-pesat-di-asean , diakses pada 9 Maret 2020

LEGAL ADAGE

LEX SEMPER DABIT REMEDIUM

The law always give a remedy