State Defense Efforts through Strengthening Cyber Law in Dealing with Hoax News

Hermina Manihuruk; Dwi Desi Yayi Tarina

Faculty of Law, Universitas Pembangunan Nasional Veteran Jakarta, Indonesia

Abstract

Geographically, Indonesia's position in the crossing of continents, between Asia and Australia, and between two oceans, the Indian Ocean and the Pacific Ocean, is a natural trajectory for trade, exploitation of marine products and military traffic. Comparable with the level of threat, Indonesia has great potential to make other interested parties not carelessly indiscriminate to divide Indonesia. Cyber law is a legal aspect whose term originates from cyberspace law, the scope of which covers every aspect relating to individuals or legal subjects who use and utilize internet technology that begins when they begin to "go online" and enter cyberspace. The government has made a special regulation regarding cyber law which is realized as Law Number 11 Year 2008 concerning Information and Electronic Transactions. Strengthening cyber law in Indonesia is essential, to strive for national defense. Not only protect the public, but also protect nationally from the threat of cyber crime. So that the creation of a tool to convince the international world, regarding the existence of strict regulations in cyber defense as an effort to defend the country to build global security.

Keywords: *State Defense; Cyber; Hoax*

Introduction

The development of globalization and information technology has brought big changes in human life. Information technology makes communication between humans and between nations easier and faster without being influenced by time and space. Globalization is a process of changing the dynamics of the global environment as a continuation of a situation that previously existed which is characterized by the characteristics of technological and information progress, causing interdependence, blurring of national boundaries (Scholte, 2000). The era of globalization has pushed some countries to stop using traditional and conventional methods of war. As a result, the power of the state is no longer seen in the strength of weapons, but also in terms of culture, economy, politics and technology. This makes competition and warfare increasingly invisible. Wars and conflicts that occur in a country are not only dominated by military forces, but non-military forces are also carried out by non-state actors.

Forms of war that no longer use traditional war methods pose new threats in cyberspace. Threats that evolve into cyber attacks are not just concepts. The vulnerability of information exchange in cyberspace is encouraged by a country to build a security system that can overcome these threats. Threats in the cyber space are dominated by non-state actors such as individual hackers, hacker groups, the activities of hackers, non-government organizations (NGOs), terrorism, organized crime groups and the private sector (such as internet companies and carried, security companies) can also threaten national defense and sovereignty. The target of cyber crime threats ever occurred in the case of wiretapping of the personal communication of the President of Indonesia and several high state officials conducted by Australia based on documents leaked by Edward Snowden, a former National Security Agency (NSA) contractor from the United States. In addition, one of the official websites of the Republic of Indonesia's Ministry of Defense (Kemhan RI) work unit was hacked, namely the website of the Directorate General of Defense Potential (Ditjen Pothan) which experienced a change in the page called defacing (Kurnia, 2015).

Risks that occur in the face of threats of cyber crime originate from within and outside the country by utilizing social, political, cultural, ideological and technological development. Many methods are used by various parties to obtain information in the National Defense Information System (Sisfohanneg). Some attacks have even been carried out, for example staging actions by defacing the site of the Director General of the Ministry of Defense. Leakage of information regarding national defense contained in Sisfohanneg can threaten national sovereignty, specifically information sovereignty. The concept of risk management in defense is an important element in analyzing how much threat impacts national defense.

In the context of facing the threat of cyber crime attacks, it cannot be solved using only the power of weapons. But it requires the integration of all national forces under the command and control of the Ministry of Defense (Lestari, 2013). The risks faced in facing the threat of cyber crime are not inferior to conventional warfare. The use of cyber technology has wide impact because it can cover various aspects of community and state life, including ideology, politics, economics, socio-cultural and security. Cyber crime is increasing which is used by certain parties individually or in groups or countries with a specific purpose to weaken their opponents. This condition needs to be watched because it does not rule out the possibility that a country can be paralyzed and destroyed by technological war or through cyberspace (Brantas, 2014).

As a sovereign and civilized nation, efforts are needed to maintain the integrity of a country by building a strong national defense in order to achieve the objectives of the national interest. The various conditions above can illustrate the importance of risk management identification in dealing with the threat of cyber crime in the management of national defense development.

In the midst of the frenetic media proclamation that tends to expose dirty and abominable practices in the field of law, it is deemed relevant to reintegrate religious morality into law (Atmoredjo, 2018). In the time dimension, what actually happens with the deterioration of law in Indonesia at the moment, cannot be separated from the development of law in earlier times (Atmoredjo, 2018). Various negative impacts and impacts of the development of the strategic environment accompanied by changing perceptions and the nature of threats to the existence and sovereignty of the nation must, of course, be taken seriously and addressed by the Indonesian people in earnest. This is important considering the advancement of science in technology, information and communication (Information and Communication Technologies-ICT) has implications for the development of modern warfare in the form of asymmetric warfare and proxy war. Therefore, one of the efforts that must be the focus of attention of all components of the nation is independence in the mastery, development and utilization of technology in various fields. In the context of building national defense and security aspects, the mastery, development and use of technology is a smart way to anticipate and face military and non-military threats (Kemhan, 2019).

The progress of science and technology has a considerable impact on human life and relations between countries. In almost a decade, the issue of cyber war has often been heard, even to the point where it is predicted to trigger tension between countries which could result in the threat of world peace. When discussing the defense of the country, it must first know the threat posed. As is the case in Law No. 3 of 2002 concerning National Defense, stipulates that threats in the national defense system consist of military and non-military threats, including cyber threats. Therefore, there needs to be an effort to deal with cyber crime, namely in the form of enforcement of cyber law as a force against cyber crime.

In statistics calculated by the Ministry of Communication and Information as a whole as of October 2019, the number of cyber attacks amounted to 1,161,590 (one million serratus sixty one thousand five hundred ninety) incidents with various kinds of data such as pornography, gambling, slander, fraud, sara, hardness or violence in children, trade in products with special rules, terrorism or radicalism, separatism or dangerous organizations, IPR, Information Security Violations, Negative Content recommended by Sector Agencies, Content that disturbs the public, Content that violates social values and culture, hoax news, extortion of content that facilitates access to negative content and normalization.

Society's dependence on information technology is increasing, so that more risks must be faced from these developments. All aspects of life, both in the current economic, social and defense systems are already dependent on the internet. Cyber law is absolutely necessary and strategic in particular to protect the community (community) which is an intellectual device (brainware), both in its position as business actors, supporting professionals and users (Napitupulu, 2019).

Some countries have now formed an Agency or Organization specifically dealing with cyber problems in the country's defense system. The United States has a United States Cyber Command (US Cybercom) under the United States Strategic Command (US Stratcom). The Treaty of Defense of the States in the North Atlantic or NATO established the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) as a cyber security agency in order to enhance NATO's cyber defense capabilities. Other countries in the Asian Continent and Australia also see serious problems and possibly influence national defense. Australia through the Australian Defense Department's Signal Defense Directorate forms a Agency called the Cyber Security Operations Center (CSOC) which is responsible for detecting and counteracting threats of cyber crime against Australian interests and the government. The Chinese state helped form a cyber army. The force was given the name "Blue Army", this force was tasked with protecting the country's defense against cyber attacks. The force has a homebase in the Guangzhou military region, south of China. Britain also built a cyber defense. This system, called the Cyber Security Operations Center (CSOC), is located at the UK Government Communications Headquarters (GCHQ), in Cheltenham, about 160 kilometers northwest of London.

Based on this, it was explained that the virtual world for most developed countries in this case the super power countries and great power countries such as the United States, Britain, Russia, China, Australia and other countries, became the new mandala of war that made all countries strive to strengthen its cyber defense in order to guarantee the country's sovereignty in the cyber realm. The Indonesian state adheres to the Universal Defense System. National Defense is aimed at guaranteeing the sovereignty of the country, the territorial integrity of the Unitary State of the Republic of Indonesia and ensuring the safety of the entire nation and state of Indonesia, where cyber threats constitute a form of real threat that can interfere with the achievement of state objectives as stated in the Preamble to the 1945 Constitution. Universal Defense needs to be formulated comprehensively and synchronized with the relevant Ministries / State Institutions so that the development of threats that occur can be anticipated properly.

Theoretical Review

State Defending is a reflection of the attitudes and behavior of citizens imbued with their love for the Republic of Indonesia based on Pancasila and the 1945 Constitution. In state defense education is very important because it is considered relevant and strategic, in addition to fostering national defense it is also useful to increase understanding and understanding the cultivation of the soul of patriotism and love of the motherland, so it is fitting for national and state awareness to be developed and developed throughout the whole community.

Understanding the defense of the State when viewed from 2 (two) aspects or angles can be described as follows:

a. Literally (based on language, defending the State can be interpreted as an effort to defend the State (from all threats, dangers and other negative possibilities).
b. Contextually (based on real situations and conditions in national and state life) and operationally (based on the form of its implementation in the field), defending the State can be interpreted as an effort made by all elements of the nation in order to protect, protect and defend the country from various threats, disturbances, attacks and other dangers, both coming from within the country and from abroad.

Some sources of literature and legislation classify the defense of the State as an attitude and behavior that is loyal and willing to sacrifice for the nation and the State. In this context, defending the State is defined as the attitudes and behavior of citizens imbued with a love for the Unitary State of the Republic of Indonesia (NKRI) based on the Pancasila and the 1945 Constitution in maintaining the survival of the nation and the State as a whole.

In the modern era and globalization today, defending the State is increasingly complex. In the midst of such situations and conditions, defending the State is not only related to one or several things, but is related to many things that are of State interest. Matters referred to include, among others, the State's territory, national defense, human resources, natural resources, artificial resources, national facilities and infrastructure, mobilization, and demobilization. Understanding of these terms include:

a. Citizens are citizens of a country determined based on laws and regulations.
b. National Defense is all efforts to maintain the sovereignty of the State, the territorial integrity of the Unitary Republic of Indonesia (NKRI) and the safety of all nations from threats and disturbances to the integrity of the nation and the State.
c. Human resources are citizens who are psychologically and physically able to be nurtured and prepared for their ability to support the components of the country's defense force.
d. Natural resources are the potential contained in the earth, water and aerospace, which in their original form can be utilized for the benefit of national defense.
e. Artificial resources are natural resources that have been used for the benefit of the country's defense.
f. National facilities and infrastructure are the results of human cultivation which can be used as a supporting tool for the interests of national defense in the framework of supporting national interests.
g. Mobilization is the act of mobilizing and using simultaneously human resources, natural resources, and artificial resources as well as national facilities and infrastructure as a national defense force.
h. Demobilization is the act of stopping the deployment and stopping the use of human resources, natural resources, and artificial resources as well as national facilities and infrastructure simultaneously which applies to the entire territory of the State which is held in stages to restore the functions and duties of each element such as the entry into force of mobilization.

From the understanding of the defense of the State, it can take several formulations as elements and the nature of the defense of the State. Martial Arts is a must and demand for citizens. State Defense is also a vehicle for citizens to show their love and devotion to the nation and the State so that the defense of the State is at the same time a right of citizens. As an effort, defending the State is carried out as a form of defense to maintain the sovereignty, existence and survival of the nation and the State.

The elements and nature of the defense of the State can be broken down into the following formulations:

a. Defending the State is a guided and coordinated effort. State Defending is carried out with leadership and coordination of the State defense and security apparatus (TNI and Polri).
b. Defending the State is done to defend the country from all threats, disturbances, and dangers. Threats of disturbances and dangers that arise can take various forms.
c. Defending the State is carried out by all components of the nation and the State. Basically, all citizens are required to participate in efforts to defend the State in accordance with their respective roles and positions.
d. Defending the State is done as a form of love for the nation and the State Volunteering in the defense of the State is usually based on a love for the nation and the State.
e. Defending the State is an inseparable part of national and state life. Awareness in the nation and state encourages the birth of policies on the importance of defending the State.
f. Defending the State is both an obligation and a right for citizens. As an obligation, defense is a demand for responsibility for citizens; As for rights, the defense of the State has become a vehicle for expressing love for the motherland.

Technology is an activity that is born by humans by planning and creating material objects of practical value, such as cars, planes, television, which are the results of technological development. Judging from the function and importance of technology, all circles of society and government agencies are very dependent on technology used both for positive and negative things. The word cyber and technology are elaborated from the origin of the word technique, from the Greek word Technikos which means art or skill in and logos are the limo or the main principles in cyberspace (Brantas, 2014). Increased utilization of cyberspace in all lines of community life in the current era of globalization in parallel, will connect to the use of an internet technology network in certain objects or sectors in accordance with the objectives of its deployment.

Research Methodology

Literature research aims to study, examine and trace secondary data in the form of primary, secondary and tertiary legal materials.

a. Primary legal materials include:

1) Criminal Code
2) Law Number 3 of 2002 concerning National Defense
3) Law Number 11 Year 2008 concerning Information and Electronic Transactions (ITE)

b. Secondary legal materials include:

Books, journals, dissertations, research reports and papers relating to research problems.

c. Tertiary legal materials include:

Newspapers, the internet, legal dictionaries, which provide instructions and explanations for primary and secondary legal materials.

Discussion

Cyberlaw or someone who knows cyberspace law, has been known since the mid-1990s following the development of the internet. The presence of the information society is believed to be one of the important agenda of the world community in the third millennium, among others, marked by the widespread use of the Internet in various activities of human life, not only in developed countries but also in developing countries including Indonesia (Mursito, Sirait, & Wardhana, 2005). Cyberlaw is a legal aspect whose scope covers every aspect relating to individuals or legal subjects who use and utilize internet technology that starts when online starts and enters the cyber or cyberspace. The purpose of cyber law is because of the importance of preventing crime or handling the crime itself. Cyber law will be used as a strong legal basis in the process of law enforcement against crimes with electronic and computer security, including money laundering and terrorism crimes. This law law rests on previous legal disciplines including: IPR, civil law, law international law and international law. This is because the scope of cyber law is quite broad. Because at this time the development of online transactions (e-commerce) and e-government programs on June 9, 2003 after the USA E-Government Act 2002 Public Law is growing rapidly.

The internet itself is defined as a computer network that is connected internationally (Wright & Winn). In a more technical perspective, the internet is a network of networks based on TCP / IP protocols; a human community that uses and develops these protocols and a collection of resources that can be accessed through these networks (Wright & Winn). Indonesia in this case has officially had a law to regulate irresponsible people in cyberspace. The law referred to in this case is the law on Information and Electronic Transactions (UU ITE). Compared to countries that have adopted cyberlaws, Indonesia is one of the least developed countries.

The ITE Law was drafted in March 2003 by the State Ministry of Communication and Information (Kominfo). Initially, the draft ITE Law was named the Information Communication and Electronic Transaction Law by the Ministry of Transportation, the Ministry of Industry, the Ministry of Trade, and in collaboration with the University Teams in Indonesia including the University of Padjadjaran (UNPAD), the Bandung Institute of Technology (ITB) and University of Indonesia (UI). Until finally President Susilo Bambang Yudhoyono signed the manuscript of ITE Law into Law of the Republic of Indonesia Number 11 of 2008 concerning Information and Electronic Transactions. Broadly speaking, the ITE Law regulates:

1. An electronic signature has the same legal power as a conventional sign (wet ink and stamped). In accordance with e-ASEAN Framework Guidelines (recognition of cross-border digital signatures).

2. Electronic evidence is recognized as any other evidence provided for in the Criminal Code.

3. The ITE Law applies to every person who commits legal actions, both within Indonesia and outside Indonesia who have legal consequences in Indonesia.

4. Domain Name Settings and Intellectual Property Rights.

5. Prohibited acts (cybercrime) are explained in Chapter VII (Articles 27-37):

    a. Article 27 (Asusila, Gambling, Humiliation, Extortion)
    b. Article 28 (Deceptive and Misleading News, News of Hatred and Hostility)
    c. Article 29 (Threat of Violence and Scare)
    d. Article 30 (Computer Access of Other Parties Without Permission, Cracking)
    e. Article 31 (Tapping, Amending, Omitting Information)
    f. Article 32 (Transfer, Destruction and Opening of Confidential Information)
    g. Article 33 (Viruses, Making the System Does Not Work (DOS))
    h. Article 35 (Making Like Authentic Documents (phishing)).

The spread of crime cases committed within the scope of social networks cannot be equated with general crime. Because, a crime that has been committed in the scope of information and electronic transactions is a crime that has entered into the modern level, so the need for intelligence is a set of technology.

As is well known in 2018 Indonesia is rife in the event of spreading false news or often known as hoaxes. The spreading of fake news has disturbed the public and also harmed some parties related to the news. As you well know, social media is a very vulnerable container and is often used to spread hoaxes. Very many active users in Indonesia in accessing social media, causing the hoax to spread quickly. Social media has crossed the line from hierarchical interaction patterns to egalitarian, both in political and cultural space.

The definition of hoax according to hukumonline.com which has been accessed through the English Oxford Living Dictionaries page is A humorous or malicious deception. Whereas through the Language Development and Development Board website, the Ministry of Education and Culture of the Republic of Indonesia hoaxes or hoaks is hoax.

Based on research conducted previously by Atik Astrini (2017) in Transformation Journal No. 32 of 2017 entitled "Hoaxes and Crime Banality" suggests that the spread of hoaxes on social media and online media does not just happen without the underlying interests. There is an interest behind the news, both in the realm of power politics, economics (industry and business hoaxes), ideological, personal sentiment, and so forth. The rise of information containing lies, hoaxes and slander that is found in many social media and some online news portals shows the social reality that people are permissive and familiar with lies and falseness. Society loses its critical awareness. The absence of guilt and regret is shown when producing and spreading hoaxes and lies (Astrini, 2017).

With the ease of internet access, especially the use of wifi, it makes it easier for the public to receive or send news, especially without checking the truth of an information (hoax). This shows that social media is a necessity so facing it is to spread information that can guide the public to always think clearly in accordance with the norms prevailing in Indonesian society which is crystallized in the values of Pancasila (Hidayat, 2017).

The need for people to know about the factors that cause the emergence of hoaxes that cannot be accounted for by anyone and even by the makers of the hoax. The reason hoax content is widespread on social networks quickly includes:

a. Just a humor for sheer pleasure. Everyone has their own way to make themselves feel happy. With today's technological sophistication, people can do strange, rare and illogical things. But causing admiration that is funny and full of fantasy.

b. This is just an attempt to look for sensations on the internet and social media. Usually to grab the attention of more users, website owners deliberately provide hyperbole content just to seek public attention.

c. Some use it (spreading hoaxes) in order to get more profits by collaborating with individuals (Saracen case).

d. Just to join in to make it look more exciting. This is also one of the internet marketing strategies by presenting hiberbola news, so there will be more comments and likes so that it looks livelier and more lively.

e. To corner certain parties (black campaigns). This situation often occurs during the ongoing Pilkada / Pilgub / Pileg / Pilpres. That's how humans when their passions are high in their pursuit of office, as a result all means will be done.

f. Deliberately causing unrest. When a complicated situation starts to unfold, a concern arises in the community. Some people take advantage of this anxiety to reap the maximum profit. The terms are "fishing in murky waters" and "taking advantage of the narrowness".

g. here is an intention to pit sheep. This is what often happens at this time, namely the existence of a person who is not responsible for spreading hoaxes only to pit sheep without certain interests or bring down both opponents. The current political example is more about the politics of fighting sheep (Marwan & Ahyad, 2019).

The impact caused by a hoax is twofold. Impact on individuals or people who spread the hoax, credibility down and can make other people no longer trust it. The perpetrators are also threatened Article 28 paragraph 1 of the ITE Law, because they have deliberately spread false and misleading news, the penalty is a maximum sentence of 6 years or a maximum fine of 1 billion rupiah. While the impact on society can trigger disputes, commotion and discomfort in the community (Monohevita, 2017). We can recognize hoax from several things attached to it, namely:

a. The source of the news comes from parties that cannot be trusted. There are no links to official sources. The news is from a site that is not clear who is responsible, whether individuals, institutions, or others. Or from sites that cannot be ascertained whether they have sufficient credibility or good reputation.

b. The images, photos or videos used are fabricated, or not even connected to the news. For example, editing from original sources that are made only origin.

c. Use provocative sentences, so it is easy to influence the reader.

d. Contains political and SARA elements (Monohevita, 2017).

The national security paradigm has shifted to a broader aspect that is included in the guarantee of personal security of citizens. The main obligation of a country is to provide security for its citizens which include security in various cyber crimes (Napitupulu, 2019). In this case, the information system security policy is the most important in the national legal order in the form of the Cyber Law (cyber law) which regulates cyberspace activities including sanctions for malicious and harmful activities (Napitupulu, 2019). The most important information system security policy is in the legal order in force in Indonesia, namely in the case of the ITE Law and the Criminal Code. The need for strong encouragement to the public to care in using information technology. Thus, information technology crime will be reduced. By doing so, the community has helped the country's defense efforts by becoming a smart society in using or receiving information and electronic transactions.

Strengthening cyberlaw in the effort to defend the country has a strategic position. In addition to protecting the public nationally from the threat of cyber crime, cyber law is one of the tools to convince the international community that there are strict regulations in cyber defense in Indonesia. When there is a cooperation between countries in building global security, it can run in accordance with its provisions. There are values that become the view of life of the Indonesian nation, namely Pancasila needs to be

injected to the public at large doses and at the right time so that the realization of national defense is realized. This large dose can be realized by sending messages via SMS (Short Messaging Service) both using cellular networks, as well as messages through social media such as WA, Telegram, Instagram, Facebook, and so on. Submission of this message requires packaging that is more slang and uses visual images that facilitate the message delivered so that it eventually becomes habituated so that it changes behavior to conflict into mutual respect and tolerance which is a manifestation of the high awareness of the defense of the national state (Hidayat, 2017).

Humans are not formed by the environment they receive. This forming environment is what is needed to be realized immediately by elements of government who have the authority to be able to shape the personality of the people who are Pancasilais so that their actions are the implementation of the awareness of the defense of their country. The Sinergirtas ultimately requires the involvement of the Ministry of Communication and Information as a state organization that runs communication and information development. If the dissemination of text, images, videos that spread the message of coolness and avoid conflicts in accordance with the values of Pancasila by the Ministry of Home Affairs, the Ministry of Defense and other K / L / Bs certainly requires encouragement and facilities provided by the Ministry of Communication and Information to the regions by means of a more effective delivery. in accordance with the current condition of society (Hidayat, 2017).

Conclusion

Cyber law is a legal aspect whose term originates from cyberspace law, the scope of which covers every aspect relating to individuals or legal subjects who use and utilize internet technology that begins when they begin to "go online" and enter cyberspace. The government has made a special regulation regarding cyber law which is realized as Law Number 11 Year 2008 concerning Information and Electronic Transactions. Hoax news spread that occurred in Indonesia caused unrest in the community. So that not a few people who are easily provoked by redistributing news or information that can be justified or not at all. The need to understand or sort out the news is true to be sent back to others. Strengthening cyber law in Indonesia is essential, to strive for national defense. Not only protect the public, but also protect nationally from the threat of cyber crime. So that the creation of a tool to convince the international world, regarding the existence of strict regulations in cyber defense as an effort to defend the country to build global security.

References

Astrini, A. (2017). Hoax dan Banalitas Kejahatan (Studi Pustaka tentang Fenomena Hoax dan Keterkaitannya dengan Banalitas Kejahatan). *Transformasi*, 96.

Atmoredjo, S. (2018). *Hukum dalam Pelangi Kehidupan.* Yogyakarta: Lingkar Media Group.

Brantas, S. (2014). Defence Cyber dalam Konteks Pandangan Bangsa Indonesia tentang Perang dan Damai. *Jurnal Pertahanan*, 55.

Hidayat, S. (2017). Media Sosial Dan Bela Negara: Pencegahan Konflik Sosial. *Media Informasi Kementerian Pertahanan Wira*, 46.

Kemhan. (2019, December 27). *Nasionalisme Dan Bela Negara Dalam Perspektif Ketahanan Nasional*. Retrieved from Nasionalisme Dan Bela Negara Dalam Perspektif Ketahanan Nasional: https://www.kemhan.go.id/belanegara /opini/asd.

Kurnia, E. (2015). *Kesiapan Sumber Daya Manusia Teknologi Informasi (SDM-TI) Kementerian Pertahanan untuk Mengantisipasi Cyber Walfare.* Jawa Barat: Universitas Pertahanan.

Lestari, R. (2013). Manajemen Risiko terhadap Kinerja Organisasi. *Jurnal Riset Akuntansi dan Bisnis*, 13.

Marwan, M. R., & Ahyad. (2019). Analisis Penyebaran Berita Hoax di Indonesia. *Fakultas Ilmu Komunikasi, Universitas Gunadarma*, 7.

Monohevita, L. (2017). Stop Menyebarkan Hoax. *UI Lib Berkala*, 7.

Mursito, D., Sirait, R. R., & Wardhana, S. (2005). Pendekatan Hukum Untuk Keamanan Dunia Cyber serta Urgensi Cyber Law Bagi Indonesia. *Fakultas Ilmu Komputer Universitas Indonesia*, 10.

Napitupulu, D. (2019). Kajian Peran Cyber Law Dalam Memperkuat Keamanan SIstem Informasi Nasional. *Kajian Peran Cyber Law Dalam Memperkuat Keamanan SIstem Informasi Nasional*, 103.

Scholte, J. (2000). *Globalization: A Critical Introduction.* London: Palgrave.

Wright, B., & Winn, J. K. (n.d.). The Law of Electronic Commerce. *Gaithersburg New York: Aspen Law & Business*, 6.

Copyrights