Strengthening Multistakeholder Integrated Through Shared Responsibility in The face of Cyber Attacks Threat

Dararida Fandra Mahira, Dwi Suci Rohmahwatin, Nabila Dian Suciningtyas

[1]Faculty of Law, Brawijaya University, [2]Faculty of Law, Brawijaya University, [3]Faculty of Law, Universitas Brawijaya,
Jl. MT. Haryono No.169, Ketawanggede, Lowokwaru, Malang City, East Java 65145

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

Abstracts :
The development of the Internet can increase the threat to the country's roughness in cyberspace. Cybersecurity is required as protection of virtual worlds from hazard sources. Cyber defense is also required as a form of an effort to maintain cybersecurity or cyberspace. The development of Internet technology is a new challenge for defense and security strategy that must be owned by the country. Based on these facts and issues, Indonesia needs an integrated and synergistic cyber-resistance system to realize national resilience and security in the face of cyber attack threats. This research uses the normative juridical method. This research is expected to improve the cyber resistance system in Indonesia.
Keywords*; Cyber attacks, Cyberdefense and security, Internet*

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

Abstrak :
Perkembangan internet dapat meningkatkan ancaman terhadap kedaulan negara di dunia maya. Cyber security diperlukan sebagai suatu proteksi perlindungan dunia maya dari sumber-sumber bahaya. Sedangkan Cyber defense atau pertahanan dunia maya juga diperlukan sebagai segala bentuk usaha untuk mempertahankan keamanan cyber atau dunia maya. Perkembangan teknologi internet menjadi suatu tantangan baru bagi strategi pertahanan dan keamanan yang harus dimiliki oleh negara. Berdasarkan fakta dan permasalahan tersebut, Indonesia memerlukan suatu sistem ketahanan siber yang terintegrasi dan sinergis untuk mewujudkan ketahanan dan keamanan nasional dalam menghadapi ancaman serangan siber. Penelitian ini menggunakan metode yuridis normatif. Dengan adanya penelitian ini diharapkan dapat meningkatkan sistem ketahanan siber di Indonesia.
Kata Kunci; *Internet, Pertahanan dan Keamanan Siber, Serangan Siber*

Citation :
Dararida Fandra Mahira, Dwi Suci Rohmahwatin, Nabila Dian Suciningtyas. (2020). Strengthening Multistakeholder Integrated through Shared Responsibility in the face of Cyber Attacks Threat. Lex Scientia Law Review 4(1), 63-74.
Doi : https://doi.org/10.15294/lesrev.v4i1.38191

1. Introduction

Human civilization has always changed as time goes by. Discoveries bring progress for human civilization, one of which in science and technology. The advancement of science and technology brings complex implications in human life and inter-State relations. The Internet is one of the biggest discoveries in the history of human civilization since it was discovered in 1969 by a United States Government research Institute well known as the National Science Foundation (NSF) through its network development called the Advanced Research Project Agency Network (ARPANET).[1] Since October 1972, ARPANET was introduced to the public in general and gained support and grew rapidly throughout the United States, divided into two networks, There are MILNET for military and ARPANET for non-military. The two networks are called DARPA Internet and nowdays we know as Internet.[2]

The Internet,[3] as the result of science and technology development, especially in this globalization era can not be avoided by various countries, including Indonesia. The amount of usage statistics on cyberspace or the Internet by Indonesian people every year has increased. This can be seen through the results of a national survey of Internet users penetration conducted by the Association of Internet Service Provider of Indonesia (APIJII) in 2018, there are 171.17 million people using internet of 264.16 million the total population of Indonesia or 64.8% of Indonesians are Internet users. The amount increased from 2017 when 143.28 million Internet users or 54.68% of 262 million Indonesia's total population is Internet user. As for 2016, the number of Internet users in Indonesia amounted to 132.7 million people or 51.5% of 256.2 million of Indonesia's population.

Chart 1. Internet user Statistics in Indonesia year 2018

Source: APIJII

Since the existence of communication model through the cyberspace or the Internet, the conventional boundaries that previously embraced and adhered to by the

[1] Ratno Dwi Putra,*et.al*., 2018, Ancaman Siber dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta), *Journal of Asymmetric Warfare*, Volume 4, No.2, Pertahanan Indonesia *University*.
[2] Ibid
[3] *The Internet according to* Abdul Wahid *and* Mohammad Labib *in his book titled* Kejahatan Mayantara *(Cybercrime).* (2005). Jakarta : Rafika Aitama , p.32 *is also described as cyberspace or cyberspace that is a new reality or nature formed by the internet medium that creates a new society as its citizens (Netizen)*.

international consensus changed to pseudo or a borderless.[4] The strength and sovereignty of a country that previously assessed based on the perspective of economic and military power, now expanding into the mastery and utilization of Information and Communication Technology (ICT). The existence of the Internet or cyberspace is capable of penetrating various geographical barriers that not only positively impact the development of ICT but also implicates the emergence of various forms of threats to the security and sovereignty of a country (national security).

According to the Appendix of The Defence Minister of Indonesia No. 82 of 2014 concerning Cyber Defense Guidelines mentioned that cyberattack security threat is no longer reviewed from the perspective of computer security technical problems alone, it includes ideological, political, economic, social, cultural, national, military, science and technology aspects and other aspects of the life of the nation, state, and community, including personal interests that constitute national security. In the academic manuscript, the bill on security and resilience cyber mentioned that the utilization of cyberspace that no longer recognizes the boundaries of the country, making use of cyber by a party that is detrimental to the other party can be done by state actors or non-state actor who threaten state defense.

The Constitution as an Indonesian philosophical basis in living a country's life mandated through article 30 Paragraph (1) of the 1945 Constitution that every citizen has the right and must participate in the defense and security efforts of the State. Defense of the country aims to safeguard and protect the sovereignty of the country, the integrity of the territory of the unitary Republic of Indonesia, and the safety of all nations from all forms of threats as contained in article 4 of The Act Number 3 of 2002 concerning State defense. This is backed by the state defense aspect is the most essential factor in ensuring the continuity of a country to defend itself from various threats both internally and externally. The defense of the country is a manifestation of one of the country's minds contained in the opening of the Constitution of the Republic of Indonesia year 1945. There are Law protecting all nations and all the blood in Indonesia from every form of threat.

Therefore, the defense of the country must be no exception to cybersecurity threats. It is supported by cyber attack statistical data in Indonesia reported by Indonesia Security Incident Response Team on Internet and Infrastructure/Coordination Center (ID-SIRTII) in 2016 amounted to 135,672,984. The number is increased from the year 2015 which amounted to 28,430,843 attacks. A large number of cyber-attacks have not been balanced with a decent cybersecurity system. Based on the assessment of the Global Cybersecurity Index (GCI) in 2017 by the International Telecommunication Union (ITU), Indonesia obtained score 0.414 and stay in position 70 from 165 countries. Indonesia's position is considered to have not had a high commitment to cybersecurity and lagged from Indonesia's neighboring countries, which is the first rank with score 0.925 and Malaysia which reached 0.893 and was able to occupy the third.

Based on these facts and concerns, Indonesia needs an integrated and synergistic cyber-resistance system to realize national resilience and security in the face of cyber-attack threats that can harm and disrupt the nation's life and state.

This study focuses on how to realize a cyber-resistance system with a multistakeholder reinforcement concept integrated through shared responsibility.

[4] Bagus Artiadi Soewardi, Perlunya Pembangunan Sistem Pertahanan Siber (*Cyber Defense*) yang tangguh bagi Indonesia (*online*), Media Informasi Ditjen Pothan Kemhan, p.g. 31. Retrieved from : https://www.kemhan.go.id/pothan/wp-content/uploads/migrasi/admin/Cyber%20Defence.pdf

Problem Formulation

1. How cybersecurity protection problems in Indonesia?
2. How is the concept of strengthening multistakeholder integrated through shared responsibility in the face of cyber attack threats in Indonesia?

2. Research Methods

The type of research used is the research of doctrinal law or also known as normative juridical, researchers studied secondary law material.[5] The methods used in the search for legal materials in this research are through library studies and documentation, as well as from the Internet. All legal materials collected in such searches are then inventoried, classified, and analyzed based on descriptive analysis with the aim to describe the various legal issues that exist so that the correct solution to this problem is obtained.

3. Result and Discussion

3.1 Various Settlement Lines

Technology continues to run alongside global developments. The potential impacts of the Internet both from the positive and negative sides continue to increase. The Internet can encourage the country's economic growth and provide ease for its citizens to access everything. The development of Internet technology creates a new dimension of the cyber world. However, the development of the Internet also increases the threat to the country's roughness in cyberspace. The threat of sovereignty in the cyber world as a result of the development of the Internet can have implications for political, economic, and social issues in a country. Cybersecurity is necessary as protection of cyberspace protections from danger possibility. The Cyberdefense also required as an attempt to maintain cybersecurity.[6] The development of Internet technology is a new challenge for defense and security strategy that must be owned by countries.

Reviewing the events that occurred a few years back, the cyber-security owned by Indonesia is still relatively weak. There are still many crimes related to cyber-security such as hacking of customer debit card data by hackers who attempted to infiltrate the bank's customer card security system in mid-May 2014. Hacking is one of the few notes on how bad cybersecurity is in Indonesia.

The weak Indonesian cyber-defense was supported by the facts released by Internet monitoring company Akamai, where crimes in cyberspace that occurred in Indonesia increased as much as doubling. The increase made Indonesia the first position as a potential target for hacker attacks, having previously been occupied by China.

In this case, there are a total of 175 countries investigated and Indonesia becomes a country that contributes as much as 38% as the target of internet hacking traffic. David Belson of Akamai Research called this hacking action due to weak

[5] Roni Hanitijo Soemitro. (1988). Metodologi Penelitian Hukum Dan Jurimetri. Jakarta : Ghalia Publisher.
[6] Moehammad Yuliansyah Saputera. (2015). Pengaruh *Cyber Securtiy Strategy* Amerika Serikat Menghadapi Ancaman *Cyber Warfare*, *Jom FISIP* Vol 2 No 2, Oktober.

security systems against the Internet and computer networks in Indonesia, giving rise to the enormous potential of internet crime.[7]

The losses from crimes that caused by utilizing Indonesia cyberspace as contained in the CIA data, has reached 1.2% of the rate of loss due to cybercrime occurring in the world. Where it is estimated that the disadvantages of cybercrime in Indonesia touched the USD 895 billion of the total estimated losses due to cybercrime in the world reaching USD 71,620 billion as outlined in the following table:

Table 1. Cybercrime damages in the world and Indonesia

	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

Source: Meeting the cyber-security challenge in Indonesia An analysis of threats and responses A report from DAKA advisory, 2013.

When reviewing the policy on cybersecurity, the handling of crimes occurring in the cyberspace differs from the handling of other crimes. Governments are generally able to easily control and enforce laws within their country's sovereignty. However, the activities in the cyberspace or location are physically subject to change at any time.[8] The next problem when determining legal and jurisdiction options have resulted in various thoughts on how to approach the problem. One of the thoughts that arise is to put the Internet as the Fourth International space as well as Antarctica, Outer Space, and ocean.[9]

3.2 Strengthening Multistakeholder integrated through Shared Responsibility in the face of cyber attack threat

The protection of cyber defense and security in Indonesia is fairly weak. Thus, Indonesia requires a more structured and integrated system in the investigation of

[7] Siti Sarifah Alia, Ketika *Hacker* Lebih Menakutkan Ketimbang Teroris, Tidak hanya berbahaya bagi keamanan negara, tapi juga ekonomi dunia (online), Retrived from : https://www.viva.co.id/indepth/fokus/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris, Accessed on April, 4 2020 at 23.55 PM.

[8] Elizabeth Longworth. (2000). *The Possibilities for legal framework for cyberspace Including New Zealand Perspective*, *Theresa Fuentes et.al* (editor), *The International Dimesions of Cyberspace Law: Law of Cyberspace Series*, Vol.1, *Aldershot: Ashgate Publishing Limited*.

[9] D. Menthe. (1998). Jurudiction in Cyberspace: A Theory of International Space. *Michigan Telecommunications and Technology Law Review* (23 April 1998)

cyber attacks. This avoids overlap as well as miscommunication between sectoral agencies that dealing with cybersecurity.

International Telecommunication Union (ITU), provides a reference to cybersecurity rating a country in increasing its commitment to cybersecurity through the Global Cybersecurity Index (GCI) which includes five pillars:[10]

1. Legal, which is the existence of legal institutions and cybersecurity frameworks;
2. Technical is the existence of technical institutions and technology applications;
3. Organizational is concerned with the coordination between policymakers and the development of cybersecurity strategies;
4. Capacity Building, by reviewing the existence of research and development, education and training programs, as well as the availability of professional and certified apparatus;
5. Cooperation, which is the pillar measured based on the existence of a cooperation framework and information-sharing network.

Therefore, the strengthening of multistakeholder in facilitating coordination through the implementation of the principle of shared responsibility between government agencies and other non-governmental and sectoral institutions.

Chart 3. Implementation Mechanisms

Source: Creation of the author

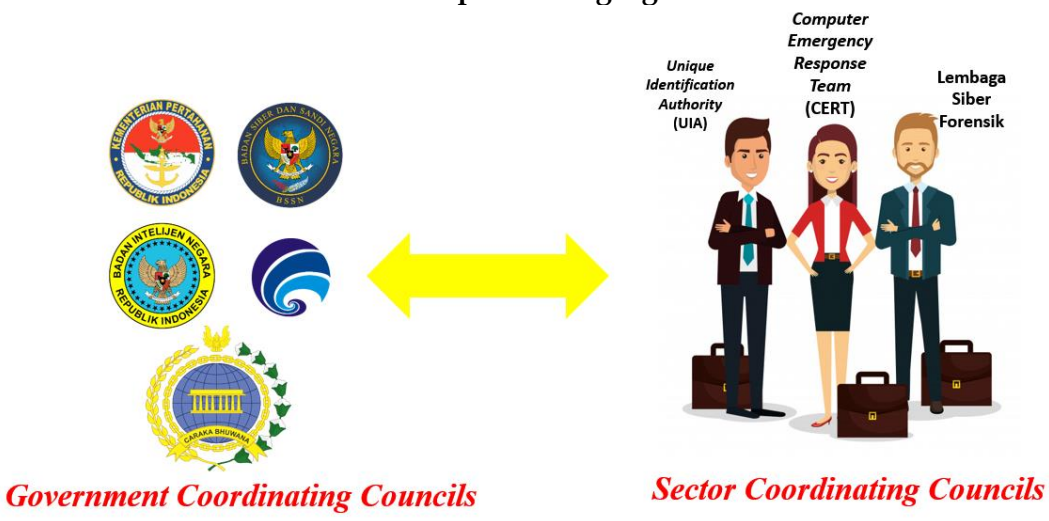
This mechanism of action is carried out through a mutually sustainable strategy, which is as follows:

[10] Maulia Jayantina Islami. (2017). Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global *Cybersecurity Index*. *Journal of Community Telematics and information* Vol 8 No 2 (Oktober Desember 2017).

1. Surveillance strategy, including monitoring of cyberspace traffic to make it easier to detect when there is a threat to cyberspace.
2. Action strategy, conducted through coordination meetings between multi-stakeholder in case of detection of cyberattacks. In this coordinating meeting, analysis related to cyber attacks occurred, then resulted in a joint agreement in the form of policy recommendations.This strategy is done as a solution to overcome the defense and security of cyberspace aimed at protecting the country from the presence of threats and cyberattacks.
3. Protection strategy, including increased cybersecurity and development of human resources to strengthen cybersecurity protection conducted through research, training, and education, as well as counseling as a form of cyber awareness. Also, another protection strategy is through information and data sharing that serves as a data center and data recovery, data network, and data protection. Through this protection strategy, facilitate the coordination of multistakeholder in conducting supervision.

Mechanism of action through the strategy is conducted based on the principle of shared responsibility among multistakeholder. The implementation of the work and mutual responsibility that is owned by this multistakeholder has functioned as a means of coordination of multistakeholder so as not to overlap the task and authority, facilitate the monitoring of cyber-space traffic, issues related to cybersecurity, the provision of cyber-related recommendations, and avoid the threat of cyber attacks that can harm the economy and threaten the sovereignty of the country. The objectives that will be achieved are to improve coordination capability between multi-stakeholders related to cyber as a protection against human rights in cyberspace as well as to ensure the resilience of the country's cyber-development where the cyber growth will be rapid.

Chart 4. Implementing Agencies



Source: Creation of the author

The principle of shared responsibility is carried out as an effort to improve cybersecurity through collaboration and integrated coordination between government agencies (Government coordinating councils) supported by other non-governmental and sectoral institutions (sector coordinating councils). The

Government, in this case, exercised functions as a maker as well as policy executor related to cybersecurity, while other sectors as supporting the cyberinfrastructure providers jointly to implement the strategy. This concept is felt to be more effective in addressing cyber-attack threats. Each institution in the Government has the following duties and authorities as follows:

1. The Indonesian National Army and the Defense Ministry of the Republic of Indonesia as the main guard in maintaining national defense enforce State sovereignty, defend the integrity of the unitary State of the Republic of Indonesia based on Pancasila and the Constitution of the Republic of Indonesia year 1945 and protect the nation from all threats and disruptions to the integrity of the nation and state by article 7 sentence (1) Act Number 34 of 2004 concerning the Indonesian National Army and article 4 of The Act Number 3 of 2002 on state defense including from threat Cyber attacks.
2. State intelligence agency as a state intelligence that has authority related to monitoring, detection, as well as cybersecurity. This is based on article 25B of Presidential Regulation Number 73 of 2017 on an amendment to presidential Regulation Number 90 of 2012 on the state intelligence agency that the state intelligence agency has a deputy field of cyber intelligence authorized to carry out activities and/or cyber intelligence operations.
3. Cyber bodies and password as institutions that perform all security tasks and functions in cyber-related information security, network and telecommunications infrastructure in the coordination of the complex cybersecurity functions by the regulation of the Presidential Decree Number 53 of 2017 on the cyber agency and the state password, wherein the provisions of article 2 shall contain the duties of the cyber Agency and the state password to implement cybersecurity effectively and efficiently by utilizing, develop and consolidate all elements related to cybersecurity.
4. The Ministry of Communication and Informatics is authorized to supervise the cyber-space traffic, detection, and protection of security networks in cyberspace. According to article 2. The Ministerial Regulation of Communication and Informatics number 26 of 2007 on the security of Telecommunications network-based internet protocol that this security is intended to support the creation of Internet network in Indonesia that is relatively free from threats and interference.
5. The Ministry of Foreign Affairs is authorized to make policies related to cooperation and diplomacy with other countries that include in the affairs of government in the field of foreign affairs by article 4 Presidential Regulation Number 56 of 2015 about the Ministry of Foreign Affairs which in this case can also be related to cybersecurity in which the representation of Indonesia in international cooperation with cybersecurity.

As the academic manuscript draft law on cybersecurity and resilience, duties and authorities owned by other non-governmental and sectoral institutions as follow as:

a. Computer Emergency Response Team (CERT), a central agent in charge of conducting technical coordination related to cybersecurity incidents. CERT serves to monitor cybersecurity threats, improve cyber awareness, and coordinate handling of incidents involving governments both at home and abroad.

b. Unique Identification Authority (UIA) is an institution responsible for the program to eliminate duplication and false identity through effective verification and authentication.
c. Forensic cyber Institution, which is the institution that conducts the investigation and analysis of data in the form of evidence found on digital devices. This forensic siber is divided into forensic computers, forensic networks, forensic applications, and forensic devices (Budi Raharjo, 384-387:2013). The Institute can collaborate with the Indonesian National Police.

This implementation will be divided into 3 (three) stages of the plan based on period, There are short-term, medium-term, and long-term. As the short-term plan in the form of the establishment of interagency Memorandum of Understanding as a manifestation of cyber protection commitment in Indonesia. This Memorandum of Understanding also contains the division of basic duties and functions of each institution to prevent the occurrence of void or spilled over authority. The medium-term plan is the establishment of presidential regulation as a legal basic. This is done because this regulation is made by the President in hopes of being kept in the related institutions, and on its formation, it does not take too long. Furthermore, a long-term plan is an increase in a legal basic by making or legalizing the Cyber Resilience and Security Act.

4. Conclusion

Internet technology continues to run in line with global developments that increase the threat to the sovereignty of the country in cyberspace. This is exacerbated by the legal condition in Indonesia that is insufficient regarding the regulation on cybersecurity. Cybersecurity must be a protection of the virtual world from danger possibility. The solution to ensuring cybersecurity by the role of a multistakeholder is integrated through the principle of shared responsibility. The purpose is to improve coordination capability among multistakeholder related to cyber as a protection against human rights in cyberspace and ensure the resilience of State cyber.

5. Acknowledgments

Authors on this occasion give a big thank you to all parties who have provided support and assistance in completing this journal to:

1. Allah SWT for His mercy to the author so that he can complete this journal;
2. A range of lecturers and staff Faculty of Law University of Brawijaya which has created a climate conducive to develop this journal writing activity;
3. Parents who have sacrificed and gave motivation to the author;
4. The partners of the legal Studies and Research Forum, the Faculty of Law of Brawijaya University, have provided invaluable support and input.

6. References

Books:

Mohammad Labib. (2005). *Kejahatan Mayantara (Cybercrime), Rafika Aitama, Jakarta.*

Roni Hanitijo Soemitro.(1988).Metodologi Penelitian Hukum Dan Jurimetri. Jakarta: Ghalia Publisher.

Journals:

Asosiasi Penyelenggera Jasa Internet Indonesia (APIJII). (2017). *Penetration information & Indonesian Internet user behavior year 2017*. Jakarta: APIJII Survey Team.

Asosiasi Penyelenggara Jasa Internet Indonesia (APIJII). (2019). *Penetration Survey Report & Indonesia Internet User Behavior Profile year 2018*. Jakarta: APIJII Survey Team.

D. Menthe. (1998). *Jurudiction in Cyberspace: A Theory of International Space, Michigan Telecommunications and Technology Law Review, 23 April,1998.*

Islami,Maulia Jayantina. (2017). *Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index, Journal of Community Telematics and information Vol 8 No 2 (Oktober Desember 2017).*

Longworth, Elizabeth. (2000). *The Possibilities for legal framework for cyberspace Including New Zealand Perspective, Theresa Fuentes et.al (editor), The International Dimesions of Cyberspace Law: Law of Cyberspace Series, Vol.1.* Aldershot: Ashgate Publishing Limited.

Rahardjo, Budi. (2013). *Sekilas Mengenai Forensik Digital, Jurnal Sosioteknologi, Issue 29, Year 12, Faculty of Fine Art and design*. Bandung:Institut Teknologi Bandung.

Ratno Dwi Putra, dkk. (2018). *Ancaman Siber dalam Perspektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta), Journal of Asymmetric Warfare, Volume 4, No.2, Pertahanan Indonesia University.*

Saputera,Moehammad Yuliansyah. (2015). *Pengaruh Cyber Securtiy Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare, Jom FISIP Vol 2 No 2, Oktober.*

Online:

Bagus Artiadi Soewardi, Perlunya Pembangunan Sistem Pertahanan Siber (Cyber Defense) yang tangguh bagi Indonesia (online), Media Informasi Ditjen Pothan Kemhan, hlm. 31, Retrieved From: https://www.kemhan.go.id/pothan/wpcontent/uploads/migrasi/admin/Cyber%20 Defence.pdf , Accessed on April 4 2020 at 23.22 PM.

Meeting the Cyber Security Challenge in Indonesia an Analysis of Threats and Responses A report from DAKA Advisory (online), Retrieved From : http://dakaadvisory.com/wp-content/uploads/DAKAIndonesia-cybersecurity-2013-web-version.pdf, Accessed on April 4 2020 at 13.30 PM.

Siti Sarifah Alia, Ketika Hacker Lebih Menakutkan Ketimbang Teroris, Tidak hanya berbahaya bagi keamanan negara, tapi juga ekonomi dunia (online). Retrieved from: https://www.viva.co.id/indepth/fokus/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris. Accessed on April 4 2020 at 23.55 PM.

Laws and Regulations :

The 1945 Constitution of the Republic of Indonesia

The Act number 3 of 2002 concerning State Defense, Supplementary State. Gazette of the Republic of Indonesia number 4169

The Act number 34 of 2004 concerning the Indonesian National Army. State Gazette of the Republic Indonesia of 2004 number 127, the addition of State Gazette of the Republic Indonesia of 2004 number 4439

The Ministerial Regulation of Communication and Informatics Number 26/PER/M. KOMINFO/5/2007 on securing the utilization of telecommunications network-based Internet protocol

The Ministerial Regulation of Defense Number 82 of 2014 concerning Cyber Defense guidelines, State Gazette of the Republic Indonesia of 2014 number 1712

E-ISSN: 2598-9685 , P-ISSN: 2598-9677

LEGAL ADAGE

COMMUNI OBSERVANTIA NON EST RECEDENDUM

There should be no daparture from common observance (or usage)