Jurnal Pertahanan
Media Informasi tentang Kajian dan Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity

P-ISSN: 2087-9415
E-ISSN: 2549-9459
Vol. 3 | No. 3

Internet Eavesdropping: Information Security Challenge in the Cyberspace

Rudy Agus Gemilang Gultom*

*Universitas Pertahanan Indonesia

Article Info

Keyword:
Civic education, Radicalism, and State defense.

Corresponding Author:
rudygultom@lemhannas.go.id

Jurnal Pertahanan
Volume 3 Nomor 3
September – December 2017
P–ISSN. 2087-9415
E–ISSN. 2549-9459
hh. 243-260

Abstract

In the era of information globalization the activity of information tapping over the Internet is one of the negative impacts of the interconnectivity between the Internet users and the ease of the process of exchanging data on the Internet. The disclosure of classified sensitive or confidential information or the loss of important documents is the result of information that is not well protected. Therefore, Internet users need to know more information about eavesdropping via the Internet to improve information security.

Di era globalisasi informasi kegiatan penyadapan informasi melalui Internet merupakan salah satu dampak negatif dari saling keterhubungan antar pengguna dan kemudahan proses bertukar data di Internet. Terbongkarnya informasi berklasifikasi sensitif atau rahasia hingga tercuri atau hilangnya dokumen-dokumen penting merupakan akibat dari informasi yang tidak terlindungi dengan baik keamanannya. Oleh sebab itu, para pengguna Internet perlu mengetahui informasi tentang penyadapan melalui Internet untuk meningkatkan keamanan informasi.

Introduction

In the current era of information globalization, the strength, sovereignty and resilience of a country is not only measured by the magnitude of military or economic power it has, but also depends on many aspects of mastery, use and empowerment of the Cyberspace and Internet access.

Many countries nowadays are highly dependent on the

utilization of the Cyberspace and the Internet especially in economic, business, academic, social, political, governmental, defense and security aspects.

Through the utilization of constructive cyberspace, nations social relations can be organize directly in a relatively short period of time without space and time constraints, whether in peacetime, crisis or war.

The cyberspace phenomenon illustrates the reality that activities in the modern society are interconnected throughout cyberspace. From the perspective of cybersecurity, the purpose of the use of internet might also be covering the misused for negative or destructive purposes by individuals with bad intention, non-state actors and state actors.

Various facilities (tools) available on the Internet can be used to disrupt, damage, and paralyze critical infrastructure to threaten the national interests of a country, including Internet wiretapping.

Lawful wiretapping activities via the Internet fall into categories related to the domain of information security and cybercrime. The terminology of tapping can be translated as a process, way, or demonstrating intention, or measures to tap (Kristian, 2013).

In the Indonesian Dictionary, wiretapping means the process, the way, the act of tapping, meaning to listen (record) the information (secret, conversation) intentionally without the knowledge of the person.

Phone tapping (or wiretapping) is the monitoring of telephone and Internet conversations by third parties, which is often done in confidential ways. Telephone conversations may be illegally recorded or monitored, either by a third party without the knowledge of the intercepted party, or recorded by one of the parties making the call. Phone tapping is strictly controlled and is generally prohibited for privacy reasons, but may also be legalized for some reason, in accordance with applicable law in the country involved.

In the midst of advances in information and communication

technology today the wiretapping conducted through out the cyber world (Internet) is greatly organized by either a state actor or non state actors to the national interest of one other country would have the potential to become a form of cyber attack is serious.

From the perspective of Indonesian National Resilience (Tannas), threats or cyber attacks can reduce Tannas condition index as measured by Asta Gatra index parameter (Eight Gatra), namely: Ideology, Political, Economy, Social Cultural, Security, Geography, Demographic and Resources Nature (SKA).

Various information security challenges via cyberspace such as hacking, wiretapping and so on cause many countries to then establish a National Cyber Agency with the single purpose to protect their national interests and resilience. Some of those institutions known are: US Cyber Command, China PLA Blue Army, Korea KISA or Israel Unit 8200 IDF. In fact, the United States through the National Institute of Standards and Technology (NIST) has defined Cybersecurity as the ability to protect or defend the use of cyberspace from cyber attacks.

In January 2015, the Government of Indonesia in preparing herself to face these cybersecurity challenges had shown the intention to establish the National Cyber Agency (BCN) which is sanctioned by President Jokowi to become the leading sector in the National Cybersecurity endavour (National Cyber Agency, 2015; Kompas, 2017).

The plan of establishing BCN was then followed up by the Government of the Republic of Indonesia with the plan to accelerate the formation of the Agency through the Coordinating Ministry of Politics, Legal, and Security of the Republic of Indonesia under the leaderhip of General TNI (Ret) Wiranto (Kompas, 2017).

In May 2017, finally the Government of the Republic of Indonesia established the official governmental agency that became the leading sector of the national cyberspace affairs through the issuance of Presidential Decree No. 53 of 2017 on the establishment of the

National Cyber and Encryption Agency (BSSN) dated May 23rd, 2017.

Moreover, Indonesia currently ranks 5 countries the largest Internet users in the world after China, India, the United States and Brazil with the number of Indonesian Internet users who reached 132.7 million users or about half of the population of Indonesia.

Understanding the Challenges of Global Information Security

To understand the cybersecurity challenges in the context of the global domain requires an understanding of the development of the global strategic environment. One country must be able to comprehend holistically that cyberspace as a borderless global domain, spaceless and timeless that bring new challenges in the current era of globalization of information.

The unconformed international understanding of the meaning of cyberspace and how go govern it will remain as obstacles, challenges and resistance when one country try to make a unilateral claim that global cyberspace as part of their country's sovereignity.

This is in contrast to the claims of the conventional sovereignty of a country which governed by the international treaties, such as UNCLOS 1982 (United Nations Convention on Law of the Sea) whereas in UNCLOS 1982 it is clearly and assertively defined the right that a sovereign state and the responsibility of a sovereign state in the use and management of the oceans of the world in which it is entitled (ZEE – Exclusive Economic Zone) and establishes guidelines for its business, environment and her natural reserves management. Sovereignty in cyberspace today are seen to be non-physical, boderless, stateless and timeless to all.

So what is border in cyberspace then explained by the Government of the United States of America through The United States Deparment of Defense (DoD) (2011) as:

"A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet,

telecommunications networks, computer systems, and embedded processors and controllers".

The US DoD then creates a definition derivative for cyberspace operations as "The employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace".

When referring to the Tallin Manual document there is a more rigid definition of cyberspace operation, ie "a cyber operation, whether offensive or defensive, that is reasonably expected cause injury or death to persons or damage or destruction to objects".

Indonesia as part of the international community will also faced the global challenges of international cybersecurity affairs, information security and codes encryption through the almost the same cyberspace it is.

This challenge may have the implications as new forms of threat to the state security such as cyber attack, cyber crime, cyber prostitution, cyber propaganda, cyber terrorism to cyber warfare.

Currently more and more emerging cyber crime action conducted by international syndicate actors through Indonesian territory because the legal formality governing cyber crime activities and the capacity of the law enforcement in Indonesia is very limited let alone the public are not too aware with the understanding of Cybersecurity in general.

The properties and characteristics of the borderless, spaceless and timeless cyber spaces make cyber crime as a form of trans national crime or transnational crime (Gultom, 2015).

The development of cyber terrorist and cyber propaganda actions by the radical groups in some countries has turned out to utilize cyber space as an effective "media of struggle".

Some of their actions are carried out through cyber space such as member recruitment, control and coordination communication systems, collection of financial resources management, including hiring hackers/crackers to cyber troops and creating their own cyber weapons.

This condition makes cyberspace as a global domain to

become a national crucial issue that needs to be correctly identified, evaluated, anticipated in order to searched for a comprehensive, integral, holistic, effective and efficient solution.

Therefore, a comprehensive understanding of the aspect of cyberspace as a global domain of the international community becomes important to be addressed correctly facing the increasingly complex and dynamic cybersecurity challenges to protect the integrity and sovereignty of the Republic of Indonesia and for one of them is in the framework of drafting the Integral, Integral and Holistic Wiretapping.

Some Great Wiretapping Cases

In the context of information security there are several examples of major cases related to intercepts that have occurred in the world and in Indonesia that has the potential to threaten the national interests of a country, among others:

1. **In 1952,** government of RI wiretaps against the US ambassador in Moscow, namely by placing an electric tapper named Chrysostom in the office of the American Ambassador.
2. **Throughout 2007 to 2009,** according to the Head of the State Intelligence Agency at the time, Lieutenant General Marciano Norman, the Australian Intelligence Agency, had intercepted telephone conversations of a number of Indonesian leaders (BBC, 2013).
3. **In 2013,** The world is overwhelmed by news of NSA leakage by former intelligence analyst Edward Snowden, who discloses various wiretapping actions by the NSA and its allies, among others:
    a. Tapping Australian Intelligence to the President of Indonesia Susilo Bambang Yudhoyono and Mrs. Ani Yudhoyono (Kompas, 2013).
    b. Tapping the NSA against the German Chancellor, Mrs. Angela Merkel.
    c. Tapping the NSA against French President Francois Hollande.
    d. Tapping the NSA against the Mexican Government.

e. Tapping the NSA against Brazilian President, Dilma Rousseff.

4. **April 2016 in Panama,** there is a "leakage" via social media of 11.5 million classified documents (2.6 terabytes files) containing sensitive data from companies around 214,000 companies in a Panama well-known service company, Mossack Fonseca. The “leaked” important secret documents are emaila (4,804,618 files), database (3,047,306 files), PDF (2,154,264 files), images (1,117,026 files), texts (320,166 files) and other formats (2242 files). Suspected "leak" of 11.5 million secret documents are done through hacking by hackers or deliberately leaked / tapped by people in Mossack Fonseca itself.
5. **October 2016 in USA**, The United States government "accused" the Russian of political hacking and wiretapping attacks related to the election of the President of the United States in 2016. According to the CIA Agency intelligence analysis concluded that the activities of Russian hackers who managed to tap the information and information system of the parties directly related to the electronic votes in the United States, although this has been denied by the Russian side. A valuable lesson to be learned from this case is the requirement for special attention to cyber security for the implementation of Presidential election or Regional Head election using the **electronic system votes.** The role of the **coding system (cryptography)** is crucial in this aspect to avoid tapping.

Methods

In this paper, the authors use qualitative case study analysis. It is an approach to research that facilitates exploration of a phenomenon within its context using a variety of data sources (Baxter and Jack, 2008). The use of case study analysis to explore the depth of the various perspectives on the complexity and uniqueness of a phenoma in ‘real life’, it is to ensures that phenomena are explored with several lens variations to be revealed and understood.

Results

Internet Eavesdropping Challenges and DPI Techniques (Deep Packet Inspection)

From some conventional wiretapping techniques that exist, as a case study the author tries to focus on wiretapping through the Internet or better known as Internet Eavesdropping, where this terminology may need to be considered in the preparation of the Draft Law on Tapping being prepared by BKD DPR RI.

Internet Eavesdropping is one of the hacking techniques via the Internet that use special tools and can only be done by certain people who have special abilities. Eavesdropping is the same as stealing data or hijack the victim's communication network that became the target directly.

In simple terms the term Eavesdropping can be likened to the term "listening in" on the Internet. To implement the action Eavesdropping this course must be able to understand well the workings of the Internet and various tools.

Commonly known, some time ago information about wiretaps made by the United States Government (NSA – National Security Agency) rife talked about various media in the world.

Edward Snowden, a former NSA analyst, leaked secret NSA documents that conduct global surveillance activities in which the American government can monitor all of its citizens' digital activities (Paramadina, 2015).

With the circulation of confidential informations the world questioned the security of information and privacy in the use of the Internet. So how do you do the tapping via the Internet?

Basically tapping is done by capturing the communication of data passing through a LAN computer network (Local Area Network) liaison. As an example if Internet A user and Internet B user communicate using a LAN network, then to tap it the tapper must capture the data communication signal passing through the path between the two users.

Data communication signals use the TCP/IP protocol (Transmission Control Protocol or

Internet Protocol) through the 7-layer OSI (Open Source Interconnection) interconnection mechanism which can be seen in Figure 1.

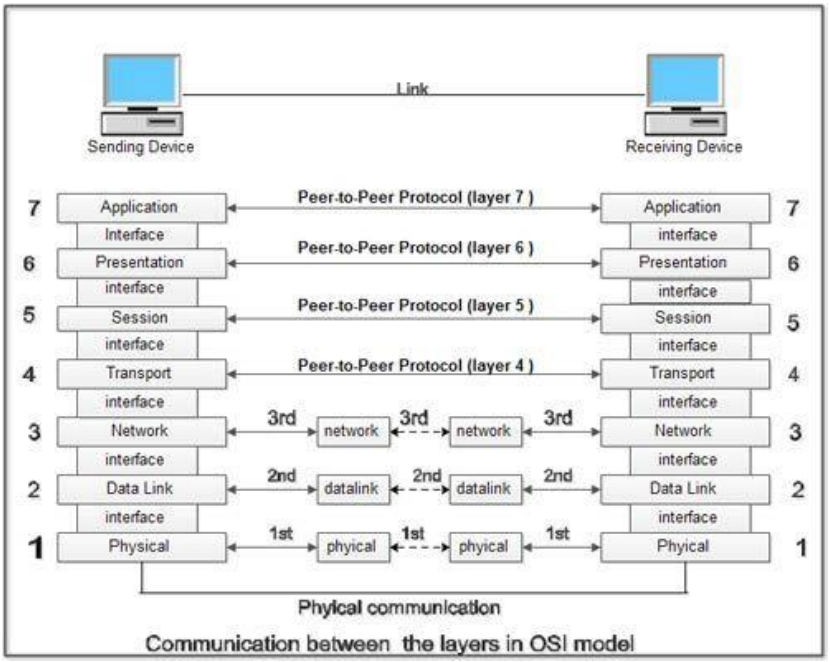

Figure 1. The 7 Layers of OSI (Open Source Interconnection)

For data types that do not have a plain text mechanism, the data signal will be "read" easily. Just as we see a collection of text that is sent of course the text will be easy to read.

While for data using security mechanisms such as encryption, the process of wiretapping would be more difficult to do, but it is still possible to do, let alone the mechanism of data communication using the mechanism of Client - Server Communication whcih always has a security holes that are open or compromised.

The other advanced techniques used to wiretapping via the Internet is to use the technique Deep Packet Inspection (DPI). DPI is simply a tapping technique performed to examine packets/data in depth (See Figure 2).

The level of depth of analysis performed in the DPI is determined by the need. DPI will be easier to do if there are supporting parameters such as origin and destination data, data types, content contained in the data, and keywords contained in the data.

These parameters will be helpful when the amount of data passing through the network is very

large. Knowing the parameters of a number of nonessential data can be passed, and only specific data will be processed and analyzed further.

DPI will be easier to do on the upstream (close to the origin of the data) and downstream (close to the destination data). Because at that position the passing data is still centered so as to minimize the data that is missed.

DPI is performed for various reasons such as improving service quality, protecting Internet users from malicious content such as viruses, to law enforcement interests. Internet wiretapping itself has actually been implemented by many countries in the World.

However, there are States that legally strictly prohibit any form of tapping to protect the privacy of its citizens. On the other hand there are also countries that implement the Internet tapping system nationally.

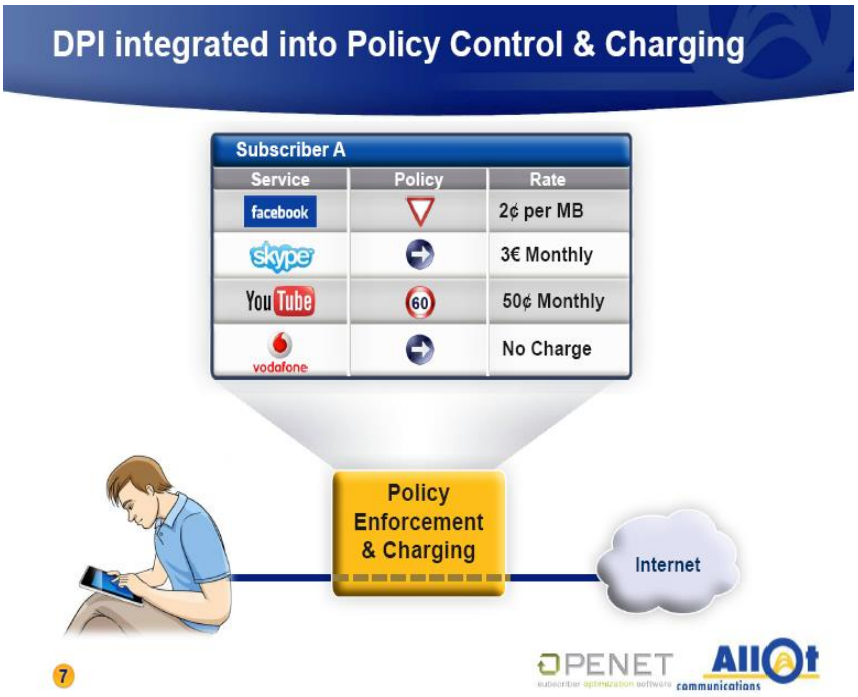

Figure 2. Policy Scheme DPI (Deep Packet Inspection)

In China, for example, we will not be able to access popular sites like google and many others (see Figure 3), due to government regulation that will include the information and access blocking known as the Great Fire Wall of China. In this case for blocking,

China will wiretap all of the data communication that will go in and out of the country. From all the data traffic in China, DPI will be exercised to filter all internet sites. Not only that, China also imposed filtering on the special keywords that are considered contrary to will create threat to their national interest.

Figure 3. The Great Fire Wall of China & DPI (Deep Packet Inspection) Policy

In Iran also applied a mechanism that is not much different with China. Iran bought Nokia Siemens Network (NSN) products that function as a national-scale DPI equipment. What the NSA does in the USA also uses basic techniques that is similar to those mention earlier.

USA has benefited from its opportunities to do wiretapping downstream of global Internet access. One of the things that lies behind it is that most of the world's Internet traffic is connected to many servers located in the USA.

Nevertheless, technical efforts to overcome the problems or at least to minimize intercepting acts have been made by some technology providers. Various protocols development have been conducted so that Internet users do not have to use or rely only to the default technology that sometimes provided by for instance a hardware producers alone.

One of the simplest tool that maybe utilized is the development of SSL (Secure Socket Layer) protocol. The public is used to use the protocol when accessing the website that begins with https.

Https is one of the SSL security protocol implementations that will encrypt/encode the data we receive and send. Another example is the implementation of Darknet.

Applications like TOR as Darknet's most popular supporters today are trying to forge the identity of Internet users and of course also encrypt their data communications.

TOR itself is actually a product of the US Navy research institution that may need to be questioned further as its credibility to ensure the confidentiality of its user information is in big doubt for the purpose of this tool when it was first established.

Another question arises how to be able to know the characteristics of an act of Eavesdroped if becomes as a victim. Some features of Internet Eavesdropping may include information when one call someone and then the voice in the call becomes discontinuous or not smoothly clear when compared to a normal call that may duet o the possibility of weak network or other disturbances by external factors during a normal and perfect network service condition on both sided.

In that instance the network experienceing a disjointed in its conncetion that this maybe a suspect of an Eavesdropping act that maybe done by a Hacker or third parties in this case. Another example of traits, maybe seen as we often get an unknown call who was asking for someone who we also do not know which we spontaneous say wrong number.

One must pay an attention to this as this may also an act of hacking underway. However, there are several ways that you can prevent an Eavesdropping, i.e to immediately change your phone number, or contact the Costumer Service phone operator and report that you suspect a strange interference on your communication number or your phone number account so the operator can do an investigation.

The perhaps best and perfect step to avoid the Eavesdropping technique is to factory reset the phone although in a case that the processor chip of the phone as been tempered with a permanent codes embeded while being produced, this technic might not be working.

Knowing the techniques and traits and countermeasures of Eavesdropping is expected, it is important to increase the awareness of all when in communication via mobile phones.

Issue Formulation

In order to draft the Bill on Wiretapping, the BKD DPR RI has been successfully formulated the main issues that exist today, among others:

1. What is the urgency of forming a draft law on wiretapping?
2. What is the definition/terminology between wiretapping, interception, and recording? What exact terminology to use?
3. Is the Wiretapping Bill addressed as a unification of various arrangements concerning wiretapping in existing legislation?
4. What is the ideal tapping procedure and interception control mechanism?
5. What are the limits that should be regulated in tapping in order not to violate human rights and in accordance with the principles of human rights protection?
6. What are the scope and content that need to be regulated in the Draft Law on Wiretapping?

Strategic Recommendations

This academic paper recommends several strategic recommendations to answer the formulation of existing problems, among others:

Firstly, the understanding that Tapping Act maybe needed to be used by law enforcement officers as one of the law enforcement tools, because Tapping is the most effective and efficient technique in surveillance and reconnaisance operation.

Tool such as DPI (Deep Packet Inspection) and others in the prevention and eradication of criminal acts need to be considered

for cases covering unussual crime (extra-ordinary crimes) such as terrorism, corruption, drugs and others.

Secondly, the Wiretapping Law should be able to regulate up to the application of the principle of Proportionality and Necessity to law enforcement officers in order to not violate human rights or misuse of authority, especially in the collection of legally valid Goods in court.

Thirdly, in the context of Internet Intercepts (cyberspace), the Tapping Act should be able to distinguish clearly and firmly the terminology of Tapping, Interception & Recording as well as the wiretapping technology used and the determination of its locus delicti in the borderless, stateless and timeless cyberspace.

Fourth, in the context of cybersecurity/information security, the Act on Wiretapping must be able to synergize with the Law on Cryptography because perpetrators of extraordinary crime criminals can utilize coding techniques in cyberspace or social media that have sophisticated end-to-end users encryption system, as an example of the use case of Telegram application in Terrorism case which made the Minister of Communication and Information of the Republic of Indonesia one time blocked the Telegram application services in Indonesia.

Conclusion

The use of violence and its effects in social life are the hallmarks of radicalism, manifested through acts of terrorism. Terrorism since the 2000 Christmas Eve bomb incidents is increasingly occurring in Indonesia to this day.

Then, defending the state is an activity undertaken by citizens is the right and obligation to defend the independence and sovereignty of the state, territorial integrity, and the safety of the whole nation from all threats.

Non-military threats or con-conventional threats such as radicalism are a new challenge in this global era for Ministry of Defence, TNI, and the Police as well, of course, as an effort to defend the country.

Every defense stakeholder in Indonesia must be involved in efforts

to eradicate radical movements, while building an effective state defense system to deal with this threat. Therefore, the state defending program should be encouraged as part of the prevention of rapid development of radical understandings.

Eradicating radical movements can not only be done by methods of repression, but how to prevent them is far more important because the spectrum is wider and has a big impact.

The state defense program is expected to change and positively influence the mindset of the Indonesian citizen so as not to be influenced by false religious doctrines and certainly also heretical.

Defend the state must be implemented seriously and comprehensively, and followed by all components of society. Effective national defense can be realized if all components of the nation have followed the defend the state program.

In order to anticipate the widespread involvement of young people in the radical ideological vortex, the state needs to consider the following points.

First, design the material and methods of defend the state that are relevant to the psychological characteristics of young people.

Second, address the dislocation and social deprivation of young people through social inclusion programs.

Third, the instilment of religious insight (religiosity) is integrated with national insight. The content of the state defending curriculum must be based on religious teachings to correct the doctrine of perverted radicalism using religious arguments.

The state defense program is a very effective program to be implemented in Indonesia in today's global era, where threats emerging are no longer of military dimension. The threat of radicalism shows us all that prevention efforts can not be done traditionally anymore, but must be done contextually.

Prevention should combine repressive actions to combat the perpetrators, but still focus on preventive methods through

dissemination of the concepts of state defense.

Reference

Badan Cyber Nasional. Plan To Establish BCN [National Cyber Agency]), http://nasional.kompas.com/read/2015/01/06/12550571/Presiden.Bahas.Pembentukan.Badan.Cyber.Nasional, downloaded on October 3rd 2017.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The qualitative report, 13(4), 544-559.

Cyber Attacks: Technique, Tools, Motivation & Impact, downloaded on October 28th 2017.

Drew, D. M., & Snow, D. M. (2006). *Making Twenty-First-Century Strategy. An Introduction to Modern National Security Processes and Problems*. AIR UNIV PRESS MAXWELL AFB AL.

Election Commission Regulation No. 12/2016 on Campaign for Regional Head Election.

Government Regulation No. 53/2010 on Disciplinary Regulations for Civil State Employees.

Gultom, Rudy. (2003). "Tantangan Teknologi Informasi Dalam Perang Modern." The Information Technology Challenge in Modern War, Kompas Newspaper, Monday, July 14th 2003.

Gultom, Rudy. (2015). "Development of the NIST Cybersecurity Framework", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, Rudy. (2015). "Cyber Conflict & Cyber Warfare," Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, Rudy. (2015). "Cyber Intelligence Overview", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, Rudy. (2015). "Cyberspace as Global Domain," Materials of Cyber Security For Information Leaders Course, The National Defense University (NDU), Washington, DC. USA, March 2015.

Gultom, Rudy. (2015). Presidential Executive Order 13636, on February 12th 2015, "Improving Critical Infrastructure Cyber" Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS), Monterey, California, USA, May 2015.

Gultom, Rudy. (2015). Presidential Policy Directive 21 (PPD-21) on 12 February 2015, "Critical Infrastructure Security and Resilience", Materials of Cyber Security Policy & Practice Course, The Naval Postgraduate School (NPS),

Monterey, California, USA, May 2015.

Kompas. (2017). Alasan Pemerintah Bentuk Badan.Cyber.Nasional (Reasons for the Government to Form National Agency.Cyber), http://nasional.kompas.com/read/2015/01/06/15464401/Ini.Alasan.Pemerintah.Ingin.Bentuk.Badan.Cyber.Nasional, downloaded on October 3rd 2017.

Law No. 10/2016 on the Election of Governor, Regent / Mayor

Law No. 11/2008 on Electronic Transaction Information (ITE).

Law No. 14/2008 on Public Information Disclosure.

Law No. 23/2014 on Regional Government.

Law No. 3/2002 on State Defense.

Law No. 5/2014 on the State Civil Apparatus.

Lemhannas RI. (2014). Strategic Review on "Indonesia Readiness Strategy Facing ASEAN Community (2015). Ditjian Internasional Debidjianstrat Lemhannas RI,

National Institute of Standard and Technology. http://www.nist.gov/ *downloaded on October 2nd 2017.*

Paramadina Foundation. (2017). "Belajar dari Kasus Edward Snowden" (Learn from Edward SnowdenCase), http://paramadina.or.id/2015/04/20/belajar-dari-kasus-edward-snowden/, downloaded on November 12nd 2017.

Pemerintah RI mempercepat pembentukan Badan Siber Nasional di tahun 2017 (The Government of Indonesia has accelerated the formation of the National Cyber Agency in the year 2017), http://nasional.kompas.com/read/2017/01/03/18063511/pemerintah.percepat.pembentukan.badan.siber.nasional.pada.2017, downloaded on October 23rd 2017.

President Obama's International Strategy for Cyberspace, "Prosperity, Security, and Openness in a Networked World", May 2011,https://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, downloaded on 3 November 2017.

Prof. Kevin P. Newmeyer, "Who Should Lead U.S. Cybersecurity Efforts?", PRISM Magazine vol. 3, no. 2, The National Defense University (NDU), Washington, DC., USA, March 2015.

Russian hacking and the 2016 election: What you need to know http://edition.cnn.com/2016/12/12/politics/russian-hack-donald-trump-2016-election/, downloaded on March 17th 2017.

The Famous Cyber Attacks/Cyber Warfare in the World," downloaded on August 20th 2017.

The Indonesian Constitution 1945.

The Tallinn Manual, "Tallinn Manual on the International Law

Applicable to CyberWarfare",https://ccdcoe.org/tallinn-manual.html, downloaded on November 12nd 2017.

The US DoD, "Department of Defense Strategy for Operating in Cyberspace", http://www.defense.gov/news/d20110714cyber.pdf, downloaded on October 27th 2017.

United Nations Convention on the Law of the Sea (UNCLOS) year 1982, downloaded on October 28th 2017.