BUILDING INDONESIA'S NATIONAL CYBER DEFENSE AND SECURITY TO FACE THE GLOBAL CYBER THREATS THROUGH INDONESIA SECURITY INCIDENT RESPONSE TEAM ON INTERNET INFRASTRUCTURE (ID-SIRTII)

Adi Rio Arianto[1] and Gesti Anggraini[2]

Universitas Pembangunan Nasional Veteran Jakarta & Universitas Satya Negara Indonesia
(arianto.adirio@gmail.com & gestianggra92@gmail.com)

Abstract – The establishment of the "Indonesia Security Incident Response Team on Internet Infrastructure (ID-SIRTII)" is a tactical step by the Indonesian Ministry of Information and Communication to ensure the stability of national information regarding cyber protection and all forms of threats. This study explores the urgency of ID-SIRTII to prevent global cyber threats. The study found that cyber threats in Indonesia are very complex, seeing the variations of actors, motives, and targets (civil or military purpose). This complexity can be explained through the following four aspects, namely : (1) by understanding of Geometripolitic studies in cyber, there are at least two domains that can be reached, namely "the using of cyber for high-politics purposes (military)"by formulating and activating of Cyberpower to face the Global Cyber War(PSG), Wold Geometri War (PGA), and the forming of "Siber State or Siber Government"; and "the use of cyber for low-politics purposes (civil)"by the protection of civil activities in cyberspace; (2) in order to prevent the spread of national cyber crime, the implementation of the ID-SIRTII policy is integrated with the national cyber institutions; (3) in order to prevent the Global Cyber Threat, the implementation of ID-SIRTII policies needs to be strengthened and well-integrated with the regional and global cyber institutions; and (4) considering of the two "functionalism of cyber" also to form a structuralism of Indonesian National Defense and Security system in the cyber sector, nowdays Indonesia needs to build a CyberForce as a complement to the Army, Navy, and Air Force.

Keywords: defense, security,cyber, ID-SIRTII, cyber force

INTRODUCTION

Twenty first century strategic environment has become part in the horizontal era (horizontalization) or Globalinium, where information safety (data, both actual and electronic) are increasingly difficult to be controlled, therefore, affecting the cyber and nuclear security.[3] In the study of International security, the terms of a horizontal era (horizontalization) or "globalinium" is introduced by Adi Rio Arianto in his work that titled "Cybersecurity towards Geometry War

[1] International Relations Study Program, Universitas Pembangunan Nasional Veteran, Jakarta. An expert in Strategy, Defence and International Security.

[2] International Relations Departement, Universitas Satya Negara Indonesia, Jakarta. Her focus of study is in strategy and international security studies.

[3] Arianto, Adi Rio. 2016. "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad 21" (Indonesian). *Proceeding in International Relations Studies National Association Convention VII* (VENNAS AIHII VII).

between Nations: Geometripolitics and the Horizontal Era World Security Architecture in the 21st Century." [4] According to Arianto through the concept of Geometripolitics, information security is part of the cybersecurity, since the method and ways to protect information are part of cybersecurity which is based on international security studies.

Regarding the threat of 21st century, the view of Raden Mas Jerry Indrawan and Efriza need to be considered, where the threat of the 21st century are intangible (unseen) in nature for example ideological threat in the form of terrorism and radicalization which have implication on the country defense and national security specifically Indonesia. [5] In this situation *intangible* threat intersects with with cyber threat because they physically have no form, but the effect can be felt. Brascomb expressed that information functioned like a human body blood system.[6] With the result that threat to the information is part of the cyber threat, and the threat to the cyber world to sure threaten the national cybersecurity followed by the threat towards global cybersecurity. In sum, the threat towards the cybersecurity is a total threat against the international security.

In regards of global cybersecurity, internet push human to be integrated with the activity of cyberspace. Internet have caused one of the largest leap in the human performance. Internet are not value free, therefore, cyber is also not value free when in touch with politics that ended with power formation. Technology witll become more effective if given strategic attention towards the utilization of technology that acustomed with values of society which are bounded with national regulation to protect society from the negative impact that emerge from it. Therefore, Cyber is absolutely controlled.

Indonesia continue to strengthen the information traffic in cyberspace effectively. Internet users in Indonesia have reach 82 millions users, putting Indonesia in the 8th place in the world in terms of active internet users. [7] This number doesn't reflect the safety of it,

---

4 *Ibid*

5 Raden Mas Jerry Indrawan and Efriza, "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia", *Jurnal Pertahanan dan Bela Negara* (*Indonesian*), Universitas Pertahanan Indonesia, Number 3, Volume 7, December 2017, pp. 1-2

6 Anne W. Brascomb, *Toward A Law of Global Communication Network*, (USA: Longman, 1986), p.1.

7 For further Information could be accessed through "Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta" (Indonesian), inside of http://kominfo.go.id/index.php/content/detail/

Because Indonesia is in the position where it is weak in terms of cybersecurity. As the result pushing the cyber crime in civil realm such as the hacking of bank clients debit card which resulted from the intrusion into security system of clients card. In strategic realm (military), Indonesia is weak in terms of fortifying the information traffic. The emergence of spionage, intelligence, hacking and others case shows little about Indonesia dominance (Power) in controlling the traffic flows of Information when faced with the cyber war. This has become part of the bad record of Indonesia cybersecurity.

Furthermore, according to Akamai report shows that Indonesia cyber crimes has doubled in recent years. This number puts Indonesia in the first position in the country that potentially become the target of the hacker, replacing China.[8] These reports have also indicated that Indonesia contributed 38 percent in terms of the target of traffic hacking in Internet realm from the investigation results on 175 countries, showings Indonesia in the first place in terms of cyber crimes[9] According to a report from David Belson from Akamai research, the speed of Internet access does not always raise the potential of cyber crimes that threaten Indonesia.[10] However, the damage from the crimes that utilizes the cyberspace in Indonesia according to CIA has reached 1.20% from the liabilities that cyber crimes have created in the world, where could be seen from the Table 1.

Table 1. Estimated Loss from Cyber Crimes: Comparing Indonesia and the World

	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 Cecoming Cyber	USD 150,200 m	USD 2,748 m

Sources: DAKA Advisory, 2018[11]

3980/ Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G405R_tfs, accessed on October 24, 2018.

8 Akamai, "The State of The Internet Report", Documents of Americas Highlights, Second Quarter 2013.

9 *Ibid.*

10 "Ketika Hacker Lebih Menakutkan Ketimbang Teroris" (Indonesia), inside http://m.news.viva.co.id/news/read/507480-ketika-hacker-lebih-menakutkan-ketimbang-teroris, accessed on October 17, 2018.

11 DAKA Advisory, "Meeting the cybersecurity challenge in Indonesia An analysis of threats and responses A report from DAKA advisory", page 21, in http://dakaadvisory.com/wp-

The table above shows that the estimated loss from the cyber crimes in Indonesia is around 895 billion US dollar, which contribute around 1.20% from the total of all estimated loss by cyber crimes globally that reach 71.620 billion US dollar. In terms of policy, Cyber crimes are handled differently. A government could control and apply a law in her own territories. Whereas, cyber activity location could change as time change, or even could only be imagined.[12] According to Menthe in "*Jurisdiction in Cyberspace: A Theory of International Space*" in terms of cyber spaces, The choosing of laws and jurisdiction has resulted in different thought on how to approach the problems that resulted from Internet position as the fourth International Space, parallel with antarctic, outer spaces, and oceans. [13] Different with Arianto that put Internet (netics) as geometry space where the capabilities to form domination (power) are part of "Cybersecurity and power" that are much more complex, geometric and unlimited.[14]

Based on various views above, we need more research to deepen our knowledge in terms of complexity of cybercrimes in Indonesia, nationally, especially to understand different actor, their motives, targets and their aims which could be civil or military activity. This understanding is needed to answer four aspect below, which is : (1) How Indonesia tactical steps to support defense and security of national cybespace; *(2)* To limit the expansion of National cyber crimes, how ID-SIRTII roles strategically and the cooperation of ID-SIRTII with cyber teams and institution in national level; (3) To face global cyber threat, what steps that ID-SIRTII should take as special team to control the information traffic in cyberspaces, which included the cooperation of ID-SIRTII with regional and global cybersecurity institution (4) How urgent should Indonesia creates "Cyber Force" to create structuralism of Indonesia national cyber defense and security to complement the army, navy and air forces.

---

content/uploads/DAKAIndonesia-cyber-security-2013-web-version.pdf, accessed 22 Oktober 2018 .

12 Elizabeth Longworth, "The Possibilities for a legal framework for cyberspace- Including New Zealand Perspective", on Theresa Fuentes et.al (editor), The International Dimensions of Cyberspace Law: Law of Cyberspace Series, Vol.1, (Aldershot: Ashgate Publishing Limited, 2000), p.14.

13 D. Menthe, "Jurisdiction in Cyberspace: A Theory of International Space", *Michigan Telecommunications and Technology Law Review*, April 23, 1998, p. 59.

14 Adi Rio Arianto, 2016, *op.cit*, pp. 20-21.

DISCUSSION

Cyber Functionalism : High-Level Political Goals (Military Geometric) s Normal-Level Political Goals (Civil Geometric)

To understand the complexity of cyberspace, we need to understand more about the forms of cyber (dimension) uses as the results from the emergence of cyberspace after that to deepen the consequences that resulted from the usage of the spaces. We could call it as part of cyber functionalism. For that, Cyber Functionalism need to be researched as a philosophy of balance, power and security to form one of the cyberspace domination to supports different though on human efforts to understand causes and the effect consequences from the usage of cyberspace in the human races activity. Under this is the main concept to see the cyber functionalism which is: Geometripolitics, Telematics , Multimedia, and the Net (Netics).

First the concept of Geometripolitics. The concept of geometripolitics which also known as Arianto Theorem that found the strategic relations between: balance, power and security as part of strategic elements in power formation that involves cyber dimensions that covers: dimensions (as a virtual territory in forms of cyber), netics (electronic traffics connectivity lanes), data (a group of information virtually or electronically based), users (cyber functionalism actors), and power (domination toward data access and the complexity). These five elements is part of a requirement to form the cyber functionalism to form the cyber power (geometric). The concept of geometripolitics sees the world as a power complexity that could be grouped in 8 different dimensions which is : Land, sea, air, underground, cyber, galaxy, vacuum and equator. As for the political process that included all the dimension mentioned above, which included in here, the cyber dimension to form the International power could be called as geometripolitics or the branch of geometripolitics that surpass the branch of politics , geopolitics and astropolitics study.

From the start, power formation is formed by politics that is dominated by physical forms. Geometripolitics expanded the base of power into five different bases, which is: physical base (material), metaphysics (metaphysical), Psychologic (psychological), Ideasionic (ideational), and geometric (geometrical). Power could be formed through

geography that give birth to Geopolitics, which surpass geography through the outer spaces that gave birth to Astropolitics. As a result, geometripolitics bring out to the fourth and fifth base as a result from the birth of cyber dimension that gives birth to the power of something in the virtual world, which is the bases for ideasionic and geometrics.

Politics is dominated by a limited physical base to reach power. Whereas geopolitics optimize the physic base of geography, which is also limited to expand the power. While astropolitics try to develop the outer space as a base of metaphysics which is unlimited with the way for the control of exploration as the source of power. With the development of power and security scope, then threats also develop as our technological advance. Advancement in technology is also influencing the expansion of cyber functionalism which included the dimensions, netics, data, users and power for information in the virtual world. Therefore, the concept of geometripolitics is one of the power concept that surpass the concept of politics, geopolitics and astropolitics as a final concept that try to map the relation between balance, power and security that surpass the physical, metaphysics, psyschologic base in a way that bring out the ideasonic and geometric base as the 4^{th} and 5^{th} complementary. As for the ideasonic and geometric base try to explain the formation of power in the virtual world. The physical base is a power building that is formed by a real, touchable and limited physical object. Metaphysics base is power building that is supported by causality abstraction. Whereas the psychologic base is an abstraction of inner atmosphere that contains the effect of power. Hereafter, ideasonic base is controlled for the unlimited idea to support the power of one of the abstraction and the geometric base is unlimited virtual power foundation that is formed as the result of cyber functionalism that surpasses the actual power.

The geometric base has the effect towards all base above, as the result two scopes of geometric is born, which is : (1) Limited geometry dimension (DGT), and (2) Unlimited geometry dimension (DGTT). Limited geometry dimension is the security dimension that has form physically, can be touched by human and limited in nature because it could be reached by human physically and can be seen by the eyes. This dimension included : land, sea, air and underground. Whereas

Unlimited geometry dimension is security and power dimension that are geometric by nature and unlimited, because it cannot be touch physically, the effect could be metaphysic, psychologic and ideasonic then could be imagined and forms security for one object. This dimension included: cyber, something that as congruent as vacuum, galaxy (outer space) and equator space.

From here, cyber functionalism could be mapped accurately, Cyber become part of the eight fields of security and world power that are included in Unlimited Geometric Dimension (DGTT). Therefore, Through the idea of Geometripolitics could be defined as "Cyber is the dimension that are geometric by form and unlimited that contain a group of electronic data that are being stored and linked with netics or the computer and cybernetic network where the functionalism form powers (domination) for the creation, deletion, distribution, velocity, acceleration, deceleration, variation and data volume. Cyber nature are geometric and unlimited, because the existence cannot be touch physically, but the effect could be felt metaphysically, psychologically, ideasonic and could be imagined to form security and power for one of the objects. Cyber by nature are geometric because cyber cannot be touch but can be formed and abstracted through the power of data traffic. As for cyber unlimited because cyber cannot be limited by anything, including state and organization, except if the functionalism limit of the cyber itself, which are the capabilities to explore cyber which is limited. Therefore, because cyber is geometric and unlimited, we could draw a conclusion, "cyber is mirage space that are a reflection of the actual object.

Cyber functionalism reflects the power that happens because of the connection of physical, metaphysics, psychologic, ideasionic, and geometric base. So With the result that could be defined as "Cybersecurity is the capabilities to creates protection geometrically and unlimitedly towards all kind of virtual dimension activities, protection towards all strategic information that also included actual data transformation into electronic data that are stored and connected by netics or computer, and cybernetic network that forms the information traffic and the protection towards information quality that included provision, deletion, distribution, velocity, acceleration, deceleration, variation and data volume." Cybersecurity tries to create a situation

where the cyber actor is included in the safety condition that included protection towards the environment (dimension), organization and infrastructure (netics), assets (data), cyber actor (user) and domination of the virtual world information (power). Organization, infrastructure and cyber users asset could be the existence of appliance that is connected with computer and internet, which includes : program, application, service, telecomunication and information data that are being sent and stored in a virtual environment, which is cyberspace.

Cyber functionalism is more strategic if are linked with the formation of "power in the virtual world." Cyber functionalism is all kind of utilization of cyberspace for all kind of purpose, including to chase for unlimited power in the cyber. In the concept of geometripolitics, cyber functionalism created power over the virtual world, called with "Geometric." The geometric effect could push all kind of strategic activity in civil and military world for example : Pushing the global cyberwar (PSG), international geometric war (PGDA) and the formation of a virtual nation or the cybergovernment. Global Cyber War is a war that happens when functionalism of cyberspace meet with power purpose (military geometric) to support the war in a virtual world where the geometric effect still in the virtual world level. As for the "international geometric war" is a war that combined all dimension (DGT and DGTT) with the cyber technology and nuclear technology where the war in cyber world will become lighters that start an actual war in the actual world. [15] Virtual Nation or Cybernation is a power that is supported by unlimited geometric power in a virtual world as the result of cyber functionalism structurally by an actor that is on par with a nation and unlimited that are formed by interest to create power over electronic data totally. This is cyberpower, one of the cybergovernment. The concept of the virtual nation appears because of evolution from all power base that is: physical, metaphysics, psychologic, ideasionic, and geometric base. Cyber functionalism could form virtual sovereignty.

In the end, in the level of country policy, the concept of geometripolitics divided cyber functionalism into two main domain, which is: first, Cyber

[15] Adi Rio Arianto, 2016, *op.cit,* p. 20.

functionalism for the high-leveled politic (military geometric) which is the utilization of cyberspace that are directed towards the control and securing military activity that resulted towards cyberwar. This utilization is far more complex because included the military instrument. If not well controlled could obstruct the military action. Cyber functionalism for military geometric could be the utilization of cyberspace for creation, deterrence and protection from all kind of attack towards the cyberinfrastructure that are connected with nuclear technology, national power plant technology, maritime technology, flight and outer space technology and also attack towards all nation facility that are connected with cyber technology that are directed for cyberwar support. Secondly. "cyber functionalism in the normal-leveled politics (civil geometric): which is the utilization of cyberspace that is directed towards control and security civil society activity in cyberspace. If this functionalism is utilized wrongly could give birth towards the cybercrime such as the attack towards all civil internet facility, such as website and others, the perforated bank clients account, data theft for economic motive, private identity dissemination, crime towards all social media activity, etc. In sum, cyberspace functionalism must be controlled accurately and comprehensively that included military geometric and civil geometric.

As we continue to the next concept which is telematics, telematics or the new hybrid of technology arise because the development of cyber technology that push development in telecommunication and information technology are well connected, which we called with the terms of convergention (fusion). The fusion of telecommunication, media and information technology push the enforcement of electronic system based on cyber that we understand with the terms of net. This concept about fusion is kept developing as the cyber technology advance in the late 20-th century into the 21st century that we called as "horizontal era (horizontalization), where the revolution in industrial activity in the cyber sector that is connected with nuclear military technology. The impact of social convergent has been felt positively and negatively.[16] Cybercrime is

[16] The Center for Communication and Information Technology, Technology Research and Application Body (BPPT), *Kajian Konvergensi Teknologi Informasi dan Komunikasi* (Indonesian), (Jakarta: The Center for Communication and Information Technology, 2007), p 3

one of the negative impacts. Cybercrime needs a lot of attention, including in Indonesia. Hereafter, practitioner called media in telematics as multimedia. The development of telecommunication system infrastructure followed by improvement in the information system has the capabilities to direct society into a new space, which is the cyber space. [17] William Gibson, in his work "Neuromancer", look deeper into the integration of computer and human activities.[18]

Furthermore in the works of Ronald Thompson and William Cats Barril "Information Technology and Management" that are related with cyberspace security, there are several aspects that need to be considered in the effort to manage the sources of information technology. This management included: (1) Software such as system and application and information technology infrastructure hardware (2) The management of information contents (3) telecommunication and internet networks (4) internet and virtual space trade through internet space.[19] While the organization related to information technology system utilization there are four main points that need attention which is: Information system, organization competition, information system and organization decision making and the organization of information system utilization.

The information system must be integrated, information technology are build by the base of a system that is designed to support works, management and decision making of the organization. Information and communication technology is one of the most important components in the development of information system.[20] The management of information system resources is the next problem regarding the challenge in the development of information and communication technology. There are four main key that need the attention which is: The management of information system resources must be placed as a proses of business management, information system building, external resources information system and management of information resources,

[17] M. Arsyad Sanusi, *Hukum Teknologi dan Informasi* (Indonesian), (Bandung: Tim Kemas Buku, 2005), pp.92-93.

[18] John Vivian, *Teori Komunikasi Massa* (Indonesian), (Jakarta: Kencana, 2008), p. 264.

[19] Ronald Thompson & William Cats Barril, *Information Technology and Management*, (New York: Mc Graw Hill, 2003), p. 29.

[20] *Ibid*, pp. 200-203.

then there are several points that need some attention: (1) legal certainty in the form of cybercrime laws; (2) technical and procedural proceeding which included last user, business direct approach, service provider and software company; (3) Organization structure to avoid overlap; (4) User education which included public campaign and communication regarding newest cyber crime threats; (5) International cooperation to tackles cyber crimes.[21]

Indonesia National Defense and Security Parameter: Roles of ID-SIRTII and National Cyber Institution

Indonesia cybersecurity situation is in a dangerous and critical phase. This is the impact of the rise of global information traffic that goes into Indonesia national information network system. Observing Indonesia is in the first position as a hacker target replacing China, the information traffic becomes much more difficult to be restrained. This push a global cybercrime that can be targeted towards paralyzing national information system if not be controlled. This situation needs large attention.

To prevent the deterioration of cyber defense and security, there is a need for cybersecurity policy law. In 2007 the government released the Communication and Information Minister Ruling number 26/PER/M.Kominfo/5/2007 regarding the safekeeping of telecommunication network utilization based on Internet Protocol and then revised in the Communication and Information Minister ruling number 16/PER/M.KOMINFO/10/2010, which is renewed again in the Communication and Information Minister ruling number 29/PER/M.KOMINFO/12/2010. This ruling becomes cornerstone for ID-SIRTII. ID-SIRTII is tasked to: (1) observe, detect, and give early warning regarding threat towards internet network, (2) coordinate with national and overseas stakeholder to increase the security of Internet network, (3) Operate and develop database system of ID-SIRTII, (4) Organize network utilization catalogue, (5) giving services over threat towards security of telecommunication based on Internet protocol, (6) become contact point with institution regarding the utilization of telecommunication network, and (7) design work program for

[21] Handrini Ardiyanti, "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia" (Indonesian), *Jurnal Politica,* Vol. 5, Number. 1 , Juni 2014, p. 108.

telecommunication network security based on internet.[22]

Beside ID-SIRTII, there is also several institution and organization that also handle the internet problem. Their presence could be felt in Indonesia national level, formally or informally which Included: Board of Information and Communication Technology (Dewan TIK, established 2006), Indonesia Security Incident Response Team On Internet and Infrastructure/Coordination Center (ID-SIRTII/CC, established 2007), Indonesia Computer Emergency Response Team (ID-CERT, established 1998), Computer Security Incident Response Team (CSIRT, established 1998), Indonesia Telecommunications User Group (IDTUG, established 2004). These organizations work sectorally in handling cybercrime and are not focused on Indonesia national interest. Because of that, it is needed for one vision in perceiving cyber functionalism as well as designing structuralism in cyber defense and security.

The legal framework for Indonesian Cybersecurity law is based on Information and Electronic Transaction Law number 11 year 2008, Government Regulation regarding Enforcement of Electronic System and Transaction number 82 year 2012 and others ministry circular letter and minister regulation. Related with the effort to guarantee the legal certainty in development of cybersecurity have been done in several ways and the development of several program such as: Initiation of Law and Regulation related to Cybersecurity such as Information and Electronic Transaction Law number 11 year 2008 and Government Regulation regarding Enforcement of Electronic System and Transaction number 82 to design national framework in cybersecurity. Legality in managing cybercrime is still weak even though there is a law that forbids any kind of attack and destruction of the electronic system. But, there is still no law that specifically governs the cyber crimes and handling of cybercrime. We could see the geometric effect and no limitation of the cyber world, hence become difficult to be handled.

There are still problem in the development of Cybersecurity: (1) The low understanding of government in cybersecurity that needed the limitation in

[22] Article 9 of Communication and Information Minister Regulations Number 29/PER/M.KOMINFO/12/2010 regardings change in two regulations of Communication and Information Minister Number. 26/PER/M.Kominf, 0/5/2007 in regards to Securing the Utilization of Telecommunication Network Security based on Internet Protocol

server services that based in overseas and the importance of secured system, (2) Legality handling of attack in cyber world, (3) the pattern of incident regarding cybercrime is really fast and difficult to be handled, (4) The institution management of National Cybersecurity, (5) The low awareness that there is threat in international cyber attack that could paralyze the national vital infrastructure, (6) The weakness of our industry in producing and developing hardware in regards of information technology that creates gap that could weaken defense in cyber world.[23] This needed to be guided and raised to support the same perception and vision to regards cyber functionalism and also design some sort of national cyber defense and security.

The handling of cybercrime is still partial and widely distributed, combined with no clear coordination in handling the cybersecurity is a problem itself. The low awareness of cyber threat has impacted the paralyzation of vital infrastructure for example the Soekarno Hatta International Airport radar that is repeatedly disturbed. This opens the possibility of cyber attack that attacks the national vital infrastructure. Regarding the cybersecurity policy in Indonesia, it is needed a policy that really governs different element regarding cybersecurity which included the policies that govern the information technology system that is used. This includes the arrangement of standard document as the reference to implement all of the process involved with information security and infrastructure standard that fit with international standard to face the cyber war. The infrastructure standard included the adequate defense perimeter, *network monitoring system*, *system information and event management* that functioned to monitor different incident in the network regarding the security. And also a network security assessment that plays role in control and measurement of security.

Cooperation in Facing Global Cyber Threat: ID-SIRTII and Cyber Institution in Regional and Global Scope

With the presence ID-SIRTII, at least Indonesia has the capability to control cyber threat from national level to the global level especially in terms of controlling information quality. If not,

[23] Hasyim Gautama, "Penerapan *Cybersecurity*" (Indonesian), on http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, accessed on October 17, 2018.

there is a possibility of cyber threat form different condition. One of the facts that shows cyber crime in Indonesia is worrying. CIA data have shown that Indonesia loss in cyber crime has reached 1,20% from all of the losses of cybercrime in the world. The handling of cybercrime is different from normal crime because the scope is unlimited.

Next, there is need for complex thought in building cybersecurity. Because of that, there are several points that we must raise in here : first, how is the cybersecurity policy that exists before and after ID-SIRTII. Second, how is the level of cybersecurity after the implementation of cybersecurity that has been enacted by Indonesia. A cybersecurity policy that has been processed in Indonesia are initiated since 2007 with the formation of ID-SIRTII which is the Team that is tasked by Communication and Information Minister of Indonesia that help the observation in Telecommunication network security based on Internet Protocol.

To support the security of Information, regional and global cooperation that has been done by ID-SIRTII based on article 9 of Communication and Information Minister Ruling number 29/PER/M.KOMINFO/12/2010 in regards to the second change in Communication Minister rules change. In this article, there are important point that are related to ID-SIRTII cooperation with different institution to support cybersecurity to prevent global cyber threat that are corder in second and 6th point that sounds: "…(2) coordination with related stakeholder in national and overseas level to enforce the roles of securing telecommunication network based on internet protocol and …(6) become the contact point with the institution in regards of securing telecommunication network based on internet."

To carry out its roles, ID-SIRTI has co-operated with a regional and international cyber institution such as: first in the regional level, there is institution such as APCERT (Asia Pacific Computer Emergency Response Team). The foundation of APCERT is initiated by Indonesia Computer Emergency Response Team (ID-CERT), Japan Computer Emergency Response Team (JP-CERT), and Australia Computer Emergency Response Team (AusCERT). One of the APCERT roles becomes the "mediator" for the member countries that faced disturbance on internet traffics and its infrastructure. Secondly, at International level, there are ITU (International

Telecommunication Union) under the United Nations Structure. Indonesia cooperation with ITU ever realized in the cases of *The Five Eyes,* which is one of the espionage that is done by United States, England, Australia, Canada, and New Zealand in acquiring information through tapping the undersea communication network cable, satellite and global communication networks. This tapping activity by *The Five Eyes* is one of the most important cyber cases because it targeted the Indonesian Government key player at that time which is President Susilo Bambang Yudhoyono and his cabinet. This is dangerous and is part of the intelligence violation because it was exposed to world public eyes.

The legal framework in Indonesia now is based on Information and Electronic Transaction Law number 11 year 2008, the Government Regulation regarding Enforcement of Electronic System and Transaction number 82 year 2012 and also Minister Circular Letter and Minister Ruling. But, there is also problem-related to development of cybersecurity that is strong enough to deter problem which included : The weak understanding of state organizer regarding cybersecurity that needs service boundary when the server is overseas and there is need for the usage of *secured system;* There is also lack of legality in handling cyber attacks; the management of national cybersecurity institution that are still partially done and distributed widely with not clear coordination in handling the cybersecurity problems.

The handling of cybersecurity need to be integrated strongly and involving different institution such as : Intelligence, law enforcer, defence and security department both the defence ministry and Indonesia national army with the government as the regulator, in this case represented by Communication and Information ministry with National Code Agency which now has transformed into *Badan Siber dan Sandi Negara* (BSSN/ Nation Cyber and Code Body). To face the cyber crime that are becoming more complex, it is reasonable for Indonesia to apply cyber dimension in "national defence and security" context by presenting: (1) Development of Structural base such as creation of cyber force to complement the army, navy and air forces; (2) the development of infrastructure base such as strengthening the special satellite for cybersecurity and defence; (3) Observe the working protocol of cyber traffic that by law entering Indonesian territory, but technically still being

controlled by several telecommunication providers that have power from technology where the tools being sold are foreign technology.

Structuralism of Indonesia National Defence and Security in Cyber Sector : Cyber Forces

The Discourse about the birth of Cyber Forces that supplement the Army, Navy and Air Forces needed to be regarded positively and seriously. This is one of the challenge of Indonesia government to present strong and good quality National Cyber Defense and Security System. Besides the structural challenge, other challenges in front of us in the development of cybersecurity policy is the threat of Cyber that are "geometric and unlimited" making the handling of it not only the responsibility of National Army, Police Force, Defence Ministry of Information and Communication Ministry. One of the interesting strategies that we need to observe in facing the global cyber threat included the serious effort from a government in handling the national cybersecurity that is supported by private sectors and society in creating and implementing a risk management program to protect the telecommunication infrastructure from a cyber world in critical conditions. Private sector and society have roles in developing and maintaining the cybersecurity system.

In the end, starting from two domains of "cyber functionalism" above to create Indonesia National Defense and Security Structuralism in Cyber Sector, it is time for Indonesia to form Cyber Forces as the complementary for Army, Navy and Air Forces. Cyber Forces will become structural formation under the Indonesia Nationa Army with developing a national strategy in terms of constructing Cybersecurity in Indonesia in the future. Beside of this, Cyber Forces is visioned to finish and support the development of Information Technology development , not only in Military Sector, but also reaching the civil sector in terms of contruction national and global cyber security. These responsibilities that are taken by cyber forces are hoped to become the central controller above Nasional Information system, Information Organization Competition, Organization information decision making and information system functionalism in two domination to cooperate with other cyber institution.

CONCLUSION

Viewing the development of cyber technology in the whole world, Indonesia has become one of the most important actors in cyber information traffics of the futures. Indonesia has become the number one country that becomes the target of a hacker, replacing China. The presence of cyber functionalism in International Political Arena, Indonesia need to prepare huge agenda to support our own Cyber defense and security to deal with global cyber threats, both in a civil sector or military sectors that lead to Global Cyber War or more complex International Geometry War. Beside of this, It is important to continue the study of Geomteripolitics that resulted in cyber power that included cyber dimension inside the power with the terms of "geometric", we also need to prepare for the formation of "Virtual Country or Cyber Government." This reminds us that power could also be formed in cyberspace that are supported by cyber sovereignty. At least the formation of "*Indonesia Security Incident Response Team on Internet Infrastructure* (ID-SIRTII)", have responded these threats with the existing human and natural resources.

To prevent the global cyber threats, This study in the end have found that cyber threats in Indonesia are complicated that are a result of a different actor, motive and their target. This complexity could be explained from the four aspect, which included: (1) From the perspectives of geometripolitics study, cyber functionalism have two domain which is the high-leveled politics goals (Military geometric) that faces the formulation and activation of cyber power in facing the global cyber war, international geometry war and the complexity of virtual country and cyber government and Cyber functionalism for the normal-levelled politics goals (civil geometry)" that included in civil activity in virtual world; (2) To stop the expansion of cyber crimes, the implementation of ID-SIRTII policy must be integrated with strategic roles in national cyber institution; (3) to faces the global cyber threat, the implementation of ID-SIRTII Policy need to be integrated with regional and global institution; and lastly (4) starting from two "cyber functionalism" above and also to creates Nationa Cyber Defence and Security Structures, it is needed for Indonesia to form Cyber Forces that complement the Army, Navy and Air Forces. Cyber Forces are visioned to solve and support information technology development, not only in the military sector, but also

reaching the civil sector in constructing the national and global cybersecurity.

The four-point above at least become one of the indicators in Indonesia preparation in facing any kind of possibilities in the 21st-century International world that are dominated by cyber technology. With this , Indonesia now has become one of the most important actors in the formation of national security architecture in Horizontal Era of the 21st-century. Indonesia needs to supports globalinium and horizontalization of the world by placing cybers as one of the strategic dimension in the 21st-century. With that, the future of Global cybersecurity is depending on Indonesia.

References

Books

Brascomb, Anne W. 1986. *Toward A Law of Global Communication Network*. USA: Longman.

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

The Center for Communication and Information Technology, Technology Research and Application Body (BPPT). 2007. *Kajian Konvergensi Teknologi Informasi dan Komunikasi* (Indonesian). Jakarta: The Center for Communication and Information Technology BPPT.

Journal Article

Arianto, Adi Rio. 2017. "Cybersecurity: Geometripolitika dan Dimensi Pembangunan Keamanan Dunia Era Horizontal Abad 21" (Indonesian). *Jurnal Power In International Relations*. Universitas Potensi Utama. Vol. 1. Number.2, February.

Ardiyanti, Handrini. 2014. "*Cyber-Security* dan Tantangan Pengembangannya di Indonesia" (Indonesian). *Jurnal Politica.* Vol. 5. Number. 1 . June.

Indrawan, Raden Mas Jerry and Efriza. 2017. "Bela Negara Sebagai Metode Pencegahan Ancaman Radikalisme di Indonesia". *Jurnal Pertahanan dan Bela Negara* (Indonesian). Universitas Pertahanan Indonesia. Vol. 7. No. 3. December.

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

Sanusi, M. Arsyad. 2005. *Hukum Teknologi dan Informasi*. Bandung: Tim Kemas Buku.

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

Thompson, Ronald & William Cats Barril. 2003. *Information Technology and Management*. New York: Mc Graw Hill.

Papers

Arianto, Adi Rio. 2016. "Keamanan Siber Menuju Perang Geometri Antarbangsa: Geometripolitika dan Arsitektur Keamanan Dunia Era Horizontal Abad 21" (Indonesian). Prosiding in International Relations Studies National Assocation Convention VII (VENNAS AIHII VII).

Akamai. 2013. "The State of The Internet Report". Document of Americas Highlights. Second Quarter.

Regulation

Article 9 of Communication and Information Minister Regulations Number 29/PER/M.KOMINFO/12/2010 regardings change in two regulations of Communication and Information Minister Number. 26/PER/M.Kominf, 0/5/2007 in regards of Securing the Utilization of Telecomunication Network Security based on Internet Protocol

Website

Gautama, Hasyim, "Penerapan *Cybersecurity*" (Indonesian), dalam http://kemhubri.dephub.go.id/pusdatin/files/materi/Penerapan_Cybersecurity.pdf, accessed on October 17, 2018.

"Kemkominfo: Pengguna Internet di Indonesia Capai 82 Juta" (Indonesian), dalam http://kominfo.go.id/index.php/content/detail/3980/Kemkominfo%3A+Pengguna+Internet+di+Indonesia+Capai+82+Juta/0/berita_satker#.U9G405R_tfs, Accessed on October 24, 2018.

"Ketika Hacker Lebih Menakutkan Ketimbang Teroris" (Indonesian), dalam http://m.news.viva.co.id/news/read/507480- ketika-hacker-lebih-menakutkan-ketimbang-teroris, accessed pada October 17, 2018.