The Urgency of Defining Indonesia's National Critical Infrastructure

Anang Setiyawan
Law Faculty, Universitas Wiraraja, Sumenep, Indonesia
E-mail : anang.setiyawan.sh@gmail.com

How to cite : Anang Setiyawan. "The Urgency of Defining Indonesia's National Critical Infrastructure". *UNIFIKASI : Jurnal Ilmu Hukum*. 6(2). 2019. 164-176. DOI : 10.25134/unifikasi.v6i2.1673
Submitted : 21-02-2019 Revised : 07-11-2019 Accepted : 04-12-2019

Abstract: *Indonesia has experienced millions of cyber attacks but it has never been able to be handled properly and completely, partly because of weak policies and conventional perspectives in understanding cyber threats. A country's vital infrastructure is related to a country's national interests, so threats to vital infrastructure are tantamount to threatening Indonesia's national interests. The level of use and dependence of a country on information and communication technology is directly proportional to the level of security and defense vulnerability in a country. Communication network connectivity and information technology cause security in this domain to become a separate issue in itself. This study aims to outline the importance of Indonesia to establish a national vital infrastructure in Indonesia to prepare Indonesia to face threats in the fifth domain. Determination of national vital infrastructure is urgent because it is closely related to the determination of jurisdiction, national defense and security policies in the cyber domain. This research is a normative study using a comparative approach. The results showed that Indonesia still uses a conventional perspective in seeing the form of threats and determining national vital objects as stipulated in Presidential Regulation No. 63 the year 2014. Therefore, to face the threats of defense, security as well as national interests of Indonesia in the cyber domain, the government needs to evaluate existing policies by the modern threats, as well as to establish and define Indonesia's vital national infrastructure.*
Keywords: *national interest, security, defense, critical infrastructure, cyber threat.*

Urgensi Penetapan Infrastruktur Vital Nasional Indonesia

Abstrak: Indonesia mengalami jutaan serangan cyber namun tidak pernah dapat ditangani dengan baik dan tuntas, hal ini diantaranya disebabkan karena lemahnya kebijakan dan perspektif konvensional dalam memahami ancaman cyber. Infrastruktur vital suatu Negara sangat terkait dengan kepentingan nasional suatu Negara, sehingga ancaman terhadap infrastruktur ini sama artinya dengan mengancam kepentingan nasional Indonesia. Tingginya penggunaan dan ketergantungan suatu Negara terhadap teknologi informasi dan komunikasi berbanding lurus dengan tingkat kerentanan keamanan dan pertahanan disuatu Negara. Konektifitas jaringan komunikasi dan teknologi informasi menyebabkan keamanan di domain ini menjadi masalah tersendiri yang kompleks. Penelitian ini bertujuan untuk menguraikan pentingnya Indonesia untuk menetapkan dan mendefinisikan infratruktur vital nasional di Indonesia dalam rangka mempersiapkan Indonesia menghadapi ancaman pertahanan dan keamanan di domain kelima. Upaya penentuan infrastruktur vital nasional ini penting segera dilakukan karena berkaitan erat dengan upaya penentuan yurisdiksi, kebijakan pertahanan dan keamanan nasional Indonesia di domain. Penelitian ini merupakan penelitian normatif dengan menggunakan pendekatan komparatif. Hasil penelitian menunjukkan bahwa Indonesia masih menggunakan perspektif konvensional dalam melihat bentuk Ancaman dan menentukan objek vital nasional sebagaimana diatur dalam Peraturan Presiden No. 63 tahun 2014. Oleh karena itu, dalam rangka menghadapi ancaman pertahanan dan keamanan serta kepentingan nasional indonesia di domain cyber maka pemerintah perlu mengkaji kembali kebijakan yang ada sesuai bentuk ancaman modern dan menetapkan infrastruktur vital nasional milik Indonesia.
Kata kunci: Kepentingan nasional, keamanan, pertahanan, infrastruktur vital, ancaman siber.

INTRODUCTION

Information technology changes battles that exist in physical domains such as land, sea, air, and space by using kinetic weapons into modern wars that are in the virtual domain and use non-

kinetic weapons[1]. Cyber power has now become a major part in new war concepts and doctrines based on modern technology. Developed countries have established virtual domains as new war domains and become part of their country's sovereignty that must be maintained. Mastery of this capability makes cyber capability the most influential instrument in almost all levels of conflict because it is able to provide new techniques to increase the speed, scale and strength of military attacks[2]. Cyber attacks are considered very dangerous because they can cause various disturbances and physical impacts on humans or other objects without crossing national borders[3]. One of the main problems that arise from cyber threats is the anonymity of attacks and connectivity between infrastructure networks (both civilian and military). The Office of Science and Technology Policy underlines the danger of vulnerability due to the interconnectivity between national infrastructures, cybernetics networks are basically a combination of networks, interconnected and interdependent. Interactions between these subsystems affect overall network performance. Interactions between subsystems cannot be predicted and sequential; these interactions can be random, asynchronous, and unpredictable[4].

Currently, Indonesia has experienced millions of cyber attacks but cannot be handled properly; this is partly due to the lack of policies related to cyber threats that cause limited perspectives on existing cyber threats. Cyber threats even though the attack technique is identical but can be distinguished based on the actor, motive, and target of the attack. Some experts in analyzing cyber attacks use strict liability and target-based approaches, where both approaches require the definition of a country's critical infrastructure. Indonesia currently still uses Presidential Decree No. 63 year 2004 concerning Security of National Vital Objects. This policy still uses conventional perspectives on threats and safeguards against Indonesia's vital objects. Therefore, the government must evaluate the policy to be adapted to the current modern threat model[5].

RESEARCH METHODS

This research is a normative legal research with a statue and comparative approach.

RESULTS AND DISCUSSION

1. The Impact of Cyber Threat

The technology revolution has significantly changed the strategic security environment. The information technology application in modern society makes the security environment change rapidly and significantly, including in the defense sector. The information technology revolution brings positive impacts as well as important negative impacts to be aware of in various forms of cyber threats. Therefore, this type of threat has become the attention of many countries in the world because it is able to provide a real significant threat to the security, defense and national interests of a country.

The urgency of managing threats in this domain encourages countries to prioritize their regulatory policies and the budget provided to minimize and protect their cyber domains. For example; The UK in carrying out cybersecurity strategy to achieve the vision of "UK is secure and resilient to cyber threats, prosperous and confident in the digital world" budgeting for 1.9 Billion Pounds for 2016-2021, this budget increased from the previous amount of 860 Million Pounds to

[1] http://www.*economist*.com/node/16478792, Accessed 23 September 2018
[2] Schreier, F., 2015. On cyberwarfare. Geneva Centre for the Democratic Control of Armed Forces.
[3] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, The Law of Cyber-Attack, California Law Review 100, 2012 :817-884.
[4] Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.
[5] Setiyawan, A. (2018). Penguatan Kebijakan dan Kelembagaan National Cyber Defense dalam Menghadapi Ancaman Cyberwarfare di Indonesia (Doctoral dissertation, Sebelas Maret University).

p-ISSN 2354-5976, e-ISSN 2580-7382
https://journal.uniku.ac.id/index.php/unifikasi

carry out cybersecurity strategy for the period April 2011 - March 2016[6]. The budget amount and the increase in the budget of each period shows that cyber threats cannot be underestimated; this is also confirmed by the National Security Strategy which states that the cyber threat as a Tier One risk to United Kingdom interests. According to the British Defense Secretary, this budget is used in response to increased cyber threats through the full spectrum of cyber military capabilities to increase attack capability, military range capabilities. This defense budget is invested in sophisticated capabilities to conduct surveillance and intelligence to keep the country safe[7].

Similar to Britain, America considers that the cyber domain as a key sector of the global economy because it is able to drive the innovation and economy. On the other hand, the developments of information technology confront America with new security challenges that make cyber threats a serious and significant threat to national economy and security[8]. The Director of National Intelligence stated that the cyber threat is the number 1 strategic threat in the U.S that replace the terrorist threat that first appeared in 911[9]. The US cybersecurity budget continues to increase every year. In 2017 US cybersecurity provided $ 19 Billons which increased 35% from 2016 to $ 14 Billion. This budget is used to support a broad-based cybersecurity to secure the government, improve the security of important infrastructure and technology, invest in equipment and the future labor force and strengthen America in order to better control digital security. In particular, this budget is to encourage the Cyber security National Action Plan in order to increase the cybersecurity level in the government's digital ecosystem as a whole[10]. The chart shows that cyber threats are one of the threats to Indonesia's national defense. The chart is in line with the potential threats chart from non-state which shows that cyber threats are increasing every year.

Chart 1. Indonesian Defense Threat Map

Source : (Hikam, 2014)

Chart 2. Potential Non-State Threats

[6]Https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf
Https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf
Https://www.nao.org.uk/wp-content/uploads/2017/09/Short-Guide-to-the-Cabinet-Office.pdf Accessed 23 September 2018

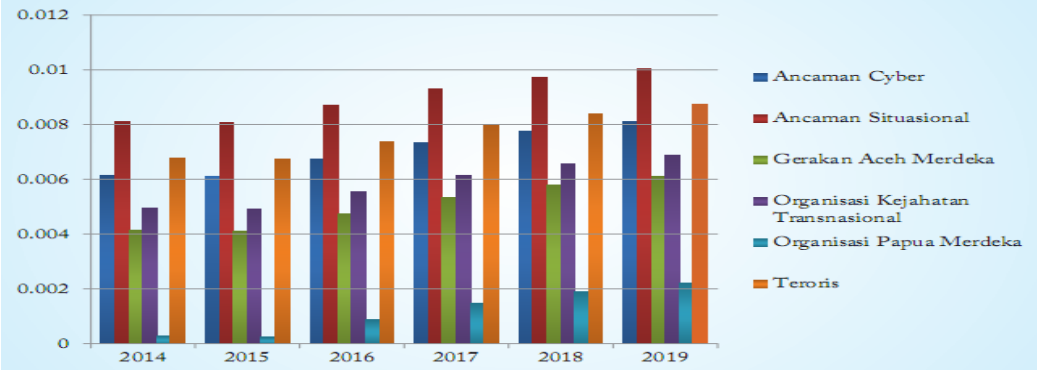
[7] Gheorghe, A. V., Tatar, U., & Gokce, Y. (Eds.). (2017). *Strategic Cyber Defense: A Multidisciplinary Perspective* (Vol. 48). IOS Press.
Janczewski, L. J., & Caelli, W. (2016). *Cyber Conflicts and Small States*. Routledge.
Https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit
Https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment
Accessed 23 September 2018

[8] International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: The White House, May 2011)
Lior Tabansky. Basic Concept in Cyberwarfare.Military and Strategic Affairs.Vol 3. No 1. May 2011. Pg 75-92.
Walters, R., 2014. Cyber attacks on US companies in 2014. Heritage Foundation Issue Brief, 4289.
Langevin, J.R., McCaul, M.T., Charney, S. and Raduege, H., 2008. Securing cyberspace for the 44th presidency. Center for Strategic And International Studies Washington DC.
Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.

[9] Carter, A., 2015. The Department of Defense cyber strategy. The US Department of Defense, Washington, DC.

[10] Budget of the United States Government, Fiscal Year 2017
Https://www.gpo.gov/fdsys/pkg/BUDGET-2017-BUD/pdf/BUDGET-2017-BUD.pdf Accessed 23 September 2018

p-ISSN 2354-5976, e-ISSN 2580-7382
https://journal.uniku.ac.id/index.php/unifikasi



Source : (Hikam, 2014)

From the data above, the government should increase awareness, speed, and accuracy in responding to various forms of threats to the Indonesian defense, including cyber threats. From the 1990s to the present, various cyberthreat cases such as cyberwarfare and cyber espionage have opened many countries' awareness of the importance of a country to be aware of cyber threats which are increasingly sophisticated and dangerous and able to influence the security and national interests of a country. The success of a cyber attack is not only measured by physical damage, but its impact on the stability, economic condition of a country and basic services to civil society such as electricity, water, transportation, communication as well as emergency services. Several cases of cyberwarfare, including:

1. North Korea's cyber attack on Sony Pictures Entertainment in November 2014 is considered as the one of the latest cyber attacks that harm American entities. This attack is destructive and also copies of unreleased films and thousands of important data containing information about celebrities, employees and Sony's business activities[11].
2. Russian cyber attacks on the Estonian information technology infrastructure network in 2007, this attack almost caused the paralysis of Estonian economic activities due to the high dependence on the use of information technology infrastructures in Estonia, including communication, banking where the majority of banking transactions in this country are run electronically[12].
3. CIA Agent cyber attacks on computer speed control pumps and gas valves worked out of control which caused Soviet-owned gas pipelines in the Siberian region to explode and were recorded as the largest explosion ever besides a nuclear bomb[13].
4. The US and NATO cyber attacks in 1998 succeeded in crippling and deceiving air defense and Serbian air traffic controllers before the bomb attack on Serbian targets in Kosovo[14]. In addition, it also blocked the Yugoslav communication network during the conflict[15]. A similar strategy was

[11] Carter, A., 2015. The DOD cyber strategy. *April*, *17*, p.2015.
https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=.6f29051f949a Accessed 23 September 2018
[12] Muhammad Saleem & Jawad Hassan, "*cyber warfare"the truth the real case, Project Report for Information Security Course*, Linköping Universitetet, Sweden
http://www.theguardian.com/technology/2007/nov/29/hacking.news Accessed 23 September 2018
[13] http://www.zdnet.com/us-software-blew-up-russian-gas-pipeline-3039147917/,
http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html,
http://www.history.navy.mil/library/online/computerattack.htm Accessed 23 September 2018
[14]Jason Porterfield, 2011.*Careers as a Cyberterrorism Expert*. The Rosen Publishing Group,
Jon Schiller, 2010. Cyber Attacks & Protection: Civilization Depends on Internet & Email, CreateSpace.
[15] K. Saalbach, Cyber War; Methods and Practice. Version 6.0-2 January 2013;1-54.

used by Israeli aircraft when attacking nuclear facilities in Syria without being detected by the air defense radar system in September 2007[16].

5. Operation Moon Maze in 1998-2000 by Russia to collect data on computer systems at the Universities, Laboratories, Pentagon, NASA and the US Department of Energy[17].
6. In 2003 China was allegedly behind the Titan Rain virus attack on America. This attack attacks computer networks of several American defense contractors such as Lockhead Martin, Sandia National Laboratories, Redstone Arsenal and even attempts to attack NASA and the FBI to retrieve their important information including army helicopter specifications, falconview (flight plan programs) and aerospace documents.

   In 2009 China allegedly carried out a systematic and large-scale cyber attack known as Operation Aurora and GhostNet. GhostNet is a large-scale espionage operation against 103 countries around the world including international organizations. This virus successfully infected 1295 computers around the world where 30% of the targets were of high value related to military, economic, political and diplomatic activities. This virus attacked several embassies including Indonesia, South Korea, Taiwan, India, Thailand, Pakistan, and Germany. This virus also attacked the Ministry of Foreign Affairs of Bangladesh, Indonesia, Bhutan, Iran, Brunei. The virus has the ability to activate and control the webcam, infected computer microphones, while Operation Aurora is used to accessing computer programs, the source code of the information technology sector, security and defense companies. in early 2011 this virus allegedly attacked the Canadian government official network which caused the Canadian government's financial department network to be offline temporarily.

   China also allegedly carried out a large-scale cyber attacks known as Operation Night Dragon and Operation Shady Rat against oil, energy and petrochemical companies and 72 organizations in the world for 6 years since July 2006.
7. Cyber attacks reportedly carried out by the US and Israel against Iran's Uranium enrichment facility program through the Stunext virus in 2010[18]. Both countries allegedly attacked Iranian and Middle Eastern Government Offices using Virus Flame which able to activate all equipment connected to computer and communication networks with spying purposes[19].
8. Cyber attacks on Saudi Aramco Oil Company companies that damage and delete sensitive data through Shamoon Malware as well as attacks on banks and television stations in South Korea that damage and delete data owned through destructive malware [20].
9. Cyber attacks after the incident between Chinese and American warplanes in 2001, provoked Chinese hackers to release the Code Red and Code Red II worm viruses which caused a loss of $ 2 million and infect 600,000 computers[21]. In 2007 and 2008 foreign countries' cyber operations were unknown to the information systems of American defense contractors; they managed to retrieve several terabytes of F-35 aircraft designs and electronic systems data. In 2011 the US

[16] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel. The Law of Cyber-Attack.California Law Review [Vol. 100:817-2012]
[17] Blakely, B. A. (2012). Cyberprints: identifying cyber attackers by feature analysis.
K. Saalbach, Cyber War ; Methods and Practice. Version 6.0-2 January 2013;1-54
[18] http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang
[19]*http://id.berita.yahoo.com/flame-serang-komputer-di-iran-dan-timur-tengah-051143829.html, http://www.pelitaonline.com/read/iptek/internasional/28/17447/virus-flame-serang-ribuan-komputer-di-iran/, http://www.antaranews.com/berita/313053/virus-the-flame-serang-iran.* Accessed 23 September 2018
[20] Kolonel (AU) Rudy Gultom, 2015, Legitimasi Badan Cyber Nasional (BCN) Sebagai Pusat Komando Dan Kendali Kerjasama Antar Instansi Di Indonesia Guna Menghadapi Tantangan Cyberspace Dan Cybersecurity Dalam Rangka Melindungi Kepentingan Dan Ketahanan Nasional, National Cybersecurity Symposium.
[21] K. Saalbach, Cyber War; Methods and Practice. Version 6.0-2 January 2013;1-54.
http://www.nytimes.com/2001/04/02/world/us-plane-in-china-after-it-collides-with-chinese-jet.html?pagewanted=all Accessed 23 September 2018

ministry stated the theft of 24,000 files consisting of data tanks, airplanes, submarines, avionics, surveillance technology, satellite communication systems, and network security protocols[22].

10. The Stunext is referred as the world's most sophisticated cyber weapon[23]. This virus was allegedly made by the US and Israel in conducting a joint operation called "Olympic Games" which was designed to infect industrial control systems, especially in SCADA automation software (Supervisory Control and Data Acquisition) (majority) made in Germany which is widely used in industrial fields[24]. This virus is estimated to have infected around 15,000-20,000 computers worldwide where the majority of infected systems are in Iranian countries, other than Indonesia, America, India, Australia, Pakistan[25]. In Iran, the virus infected Iran's nuclear facilities, causing damage to 385 centrifuges of uranium enrichment, which caused the efficiency of uranium enrichment to decrease by 30%[26]. Besides this virus infects 13,336 computers in Indonesia, 6552 computers in India, 2913 computers in America, 2436 computers in Australia, 1038 computers in the UK, 1013 computers in Malaysia and 993 computers infected in Pakistan[27]. Indonesia became the second largest country hit by this virus, but the motive and impact of the virus attack were unknown, especially to Indonesia, although this virus was also allegedly made to retrieve important information on organizational infrastructure in certain countries[28].

These cases show how cyber attacks can be used systematically to disrupt and weaken the defense systems, public infrastructure systems, economic systems, and other national vital infrastructure networks related to the safety and security of a country. In addition, cyber attacks cause high economic losses and increase every year. According to cybersecurity ventures, in 2017 global economic losses due to cyber attacks of $ 3 Trillion are predicted to reach $ 6 Trillion every year starting in 2021. This loss count includes damage and data destruction, lost productivity, stolen money, theft of personal and financial data, fraud, theft of intellectual property, embezzlement, post-attack disruption, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm[29]. In a report in 2017, the Cost of Cybercrime Study conducted by the 2017 institute phenomenon in seven countries including America, Germany, Japan, Britain, France, Italy, and Australia shows America is at the top of the country experiencing the highest losses with average losses. Annually reaching $ 21 million and Australia in the lowest position with annual average losses of $ 5.41 Million[30]. From the study, the value of losses experienced by industry shows that the financial services sector ranks top followed by utilities and energy then aerospace and defense.

---

[22] Chen, T.M., 2013. An assessment of the department of defense strategy for operating in cyberspace. Army War College Carlisle Barracks Pa Strategic Studies Institute.

[23] Lindsay, J.R., 2013. Stuxnet and the limits of cyber warfare. Security Studies, 22(3), pp.365-404. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/, http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T&r=US&IR=T, http://newatlas.com/south-korea-stuxnet-cyber-weapon/30977/ Accessed 23 September 2018

[24] http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang, http://www.news.com.au/technology/online/security/alex-gibney-film-gives-chilling-insight-into-the-world-of-state-sponsored-cyber-warfare-unleashed-by-stuxnet/news-story/a7063ae03dcb5cd6ed2a576d6a8ea9dc, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet Accessed 23 September 2018

[25]http://teknologi.news.viva.co.id/news/read/166993-trojan-scada-hantui-iran-indonesia-india, http://www.antaranews.com/berita/222505/apa-itu-stuxnet Accessed 23 September 2018

[26]Michael Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities.Submitted as coursework for PH241, Stanford University, Winter 2015

[27] Richardson, J., 2011. Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. J. Marshall J. Computer & Info. L., 29, p.1.

[28] http://teknologi.news.viva.co.id/news/read/166993-trojan-scada-hantui-iran-indonesia-india Accessed 23 September 2018

[29] https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf Accessed 23 September 2018

[30]https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf Accessed 23 September 2018

In Indonesia in 2012 to 2014 the economic losses incurred reached Rp. 33,299 billion[31] and increased to Rp. 194.6 billion from 2015 to 2016 and this number will increase every year[32]. The cyber attacks impacts should be a future lesson in dealing with potential cyber threats that are far more dangerous and complex. The attack shows clearly how cyber attacks can be used systematically, effectively and efficiently in weakening, disrupting systems related to defense, security, economic conditions and political conditions of a country. There are no politically motivated cyber attacks on Indonesia that can be handled properly and only a few attacks on economically motivated cases that can be handled indicate ineffective policies and institutions that should be able to deal with these complex threats. Therefore, the government immediately takes steps to deal with cyber threats which are increasingly sophisticated, systematic and more dangerous. This effort is carried out by strengthening the policy and integrated institutions in addressing cyber threats in the future. Weak policies create a lot of legal loopholes so that the handling of cyber threats becomes ineffective and often misguided because there are no separate domains of enforcement and handling of threats and "unknown" levels of cyber attacks on Indonesia. The weakness of the existing policies also influences the narrow viewpoint, which leads to the weakness of the relevant institutions that are authorized to handle cyber threats. Cyber domain is multidomain of almost all institutions related to Indonesia's defense, security and national interests. Therefore this domain must be managed by many relevant institutions because of its multispectrum nature. Furthermore, the international convention is required to regulate cyberwarfare by developing the existing international law principles or by expanding the definition and scope of conventional war provisions. This provision will harmonize the perspective and understanding in order to minimize debate and interpretation so that it can provide maximum protection to the population and civilian objects.

2. Cyberattack Analysis Apporach

To analyze the use of non-conventional weapons there are three models of analysis, including; Instrument based, Consequence-based and Strict Liability[33]. The instrument-based approach views whether damage/harm/destruction caused by a previous attack method can be obtained by kinetic attacks. For instance cyber attacks to disable electricity networks are automatically qualified as armed attacks because in general to disable the electricity network is carried out by dropping bombs on power plants. According to the consequence-based approach, equating cyber attacks with kinetic attacks is irrelevant and attention should be focused on the cyber attacks impact on the country. Such as cyber attacks to manipulate banking and economic service information so that disrupting trade in a country can be declared an armed attack. Manipulating information is not same as the kinetic attack but if the consequences can disrupt a country's economic activities it is considered as armed attack. According to the strict liability approach, cyber attacks on vital infrastructure are automatically considered as armed attacks. This approach was proposed by W.G. Sharp to justify the anticipation of "self-defense" before the harmful/dangerous impacts arise from the potential of cyber attacks. He stated that "... the penetration by the state into sensitive computer systems such as command and control systems, missile defense computer systems, and other computers that maintain the safety and reliability of a nuclear stockpile, should be by their very nature be presumed a demonstration of hostile intent ... "[34]. Duncan Holis uses 3 approaches to determine when a cyber attack can be called the use of armed force. First, the "instrumentality approach" approach, which argues that cyber

[31] https://inet.detik.com/security/d-3081840/kerugian-akibat-kejahatan-cyber-tembus-usd-150-miliar Accessed 23 September 2018
[32] https://www.merdeka.com/teknologi/ini-jumlah-kerugian-finansial-korban-kejahatan-cyber.html Accessed 23 September 2018
[33] Kazinec, D., 2011. Issues of cyber warfare in international law (Doctoral dissertation, Mykolas Romeris University).
[34] Elin Jansson Holmberg, armed attack in cyberspace: do they exist and can they trigger the rights to self defense?.Thesis.Stockholm University. 2015

attacks cannot be categorized as armed attacks in accordance with article 2 (4) because they do not have physical characteristics associated with military attacks. Second, the "target-based approach", that cyber attacks are considered as armed attack if the attack penetrates the vital national infrastructure system even though the attack does not cause physical harm or loss of life. According to him, this is an inclusive approach because the nature of cyber attacks has a broad impact. Third, "consequence approach", this approach emphasizes on the consequence of cyber attacks. Cyber attacks that are intended to have an impact that is usually generated by kinetic power can be referred to as an armed attack. According to Sharon, this approach does not take into account the damage caused by cyber attacks which, despite causing little physical damage. He states that; "A cyber attack that shuts down any part of a nation's critical infrastructure may have an effect that is much more debilitating than a traditional military attack. The threat in such a situation may be more terrorizing and harmful than a traditional armed attack[35].

3. Critical Infrastucture Definition in several countries

Indonesia does not use the term "vital infrastructure" but uses the term "national vital object". Presidential Decree No. 63 year 2004 defines national vital objects as areas/locations, buildings/installations and/or businesses that related to life sustainability, the state interests and/or strategic resources of state income. Included in the category of national vital objects are objects that produce daily basic needs; threats and disturbances to it result in casualties against humanity and development; threats and disturbances to it result in national transportation and communication chaos; and/or threats and disturbances to it result in disruption of the administration of government. The definition is still very limited and uses a tangible point of view, even though national vital objects have broad categories. This affects the security model and response of the authorities if there is a cyber attack on the national vital object. Infrastructure can be referred to as a vital infrastructure if the disruption to the infrastructure can result in a significant socio-economic crisis and potentially undermine the stability of a society, causing a political, strategic and security impact. There are three factors used to define vital infrastructure, namely; *the symbolic importance of the infrastructure*, *the immediate dependence on infrastructure* and *the complex dependencies*[36]. To define national vital objects, we can compare several definitions of vital infrastructure that exist in other countries and international organizations. In comparison, the US in the Presidential Decision Directives - PPD 63 1998 defines vital infrastructure as: "Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. Critical Infrastructure include, but are not limited to, telecommunications, transportation, energy, finance and banking, water systems and emergency services, both private and governmental" [37]. The USA PATRIOT Act 2001 defines critical infrastructure as systems and assets, whether physical or virtual, so vital to the U.S that the incapacity or destruction of such systems and assets would have a debilitating impact on national economic security, national security, national public health or safety, or any combination of those matters[38]. The United States has 16 sectors which are included in the category of vital infrastructure whose assets, systems, networks both physical and virtual whose inability or damage will affect the national security, national economy, public health or safety or a combination of these impacts. In the 2013 Presidential Policy Directive / PPD-21, several sectors were included in the critical infrastructure category and appointed sector-specific agencies (SSA):

[35] Christopher D. DeLuca, he Need for International Laws of War to Include Cyber Atacks Involving State and Non-State Actors, 3 Pace Int'l L. Rev. Online Companion 278 (2013).
[36] Tabansky, L., 2011. Critical Infrastructure Protection against cyber threats. Military and Strategic Affairs, 3(2), p.2.
[37] Presidential Decission Directives/PPD-63 Year 1998 https://fas.org/irp/offdocs/pdd/pdd-63.htm diakses Januari 2018
[38] H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001

Table I. Critical Infrastructure & SSA

No	Sector	Sector Specific Agencies
1	Chemical Sector	Department of Homeland Security
2	Commercial Facilities Sector	Department of Homeland Security
3	Communications Sector	Department of Homeland Security
4	Critical Manufacturing Sector	Department of Homeland Security
5	Dams Sector	Department of Homeland Security
6	Defense Industrial Base Sector	Department of Defense
7	Emergency Services Sector	Department of Homeland Security
8	Energy Sector	Department of Energy
9	Financial Services Sector	Department of the Treasury
10	Food and Agriculture Sector	U.S. Department of Agriculture and Department of Health and Human Services
11	Government Facilities Sector	Department of Homeland Security and General Services Administration
12	Healthcare and Public Health Sector	Department of Health and Human Services
13	Information Technology Sector	Department of Homeland Security
14	Nuclear Reactors, Materials, and Waste Sector	Department of Homeland Security
15	Transportation Systems sector	Department of Homeland Security and Department of Transportation
16	Water and Wastewater Systems Sector	Environmental Protection Agency

Source : (Presidential Policy Directive 21, 2013)

According to PPD-21, The Office of Infrastructure Protection leads and coordinates national programs and policies on the security and resilience of vital infrastructure while building strong partnerships across government agencies and the private sector. This office is also responsible for conducting and facilitating vulnerability and impact assessments to help understand and deal with risks to these vital infrastructures[39]. In this PPD-21 there are 3 strategies to strengthen the security and resilience of vital infrastructure, namely; Enable effective information exchange by identifying baseline data and systems requirements for the Federal Government; Refine and clarify functional relationships across the Federal Government to advance the national unity of effort to strengthen critical infrastructure security and resilience; and Implement an integration and analysis function to inform planning and operations decisions regarding critical infrastructure[40].

Malaysia uses the term Critical National Information Infrastructure (CNII) and defines it as those assets (real and virtual), systems and functions that are vital to their nation's destruction. They will have a devastating impact on[41]:

1. National defense and security; guarantee sovereignty and independence whilst maintaining internal security.
2. National image; Projection of national image towards enhancing stature and sphere of influence.
3. Government capability to functions; maintain order to perform and deliver minimum essential public services.
4. National economic strength; Confidence that the nation's key growth area can successfully compete in global market while maintaining favourable standards of living.
5. Public health and safety; delivering and managing optimal health care to the citizen

[39] https://www.dhs.gov/office-infrastructure-protection Accessed 23 September 2018
[40] Obama, B., 2013. Presidential policy directive 21: Critical infrastructure security and resilience. Washington, DC.
[41] https://cnii.cybersecurity.my/main/about.html Accessed 23 September 2018

European Union defines Critical infrastructure as "Means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, security, safety, health, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". Critical infrastructure is defined as a European Critical Infrastructure if a vital infrastructure in a member country which if disturbed or destroyed will have a significant impact on at least 2 member countries. The significance of the impact is assessed based on cross-cutting criteria[42]. Included in the European Critical Infrastructure covers 2 major sectors and their sub-sectors, illustrated in the table as follows;

Table II. European Critical Infrastructure

Sector	Subsector	
Energy	Electricity	Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity
	Oil	Oil production, refining, treatment, storage and transmission by pipelines
	Gas	Gas production, refining, treatment, storage and transmission by pipelines & LNG terminals
Transport	Road transport	
	Rail transport	
	Air transport	
	Inland waterways transport	
	Ocean and short-sea shipping and ports	

Source : (EU Commission, 2008)

From these definitions there are several similar patterns that are used to define critical infrastructure, including that (1) protected objects are tangible and intangible (virtual, system, program) objects, (2) attacks on both objects are considered to disturb the security and national interests, (3) efforts to influence, disrupt and disable an infrastructure that is not limited to destructive attacks which are considered as attacks on the state, (4) all fields categorized as vital objects are objects related to security state, governance, supporting and sustaining the national economy, the interests of fulfilling the basic needs of the people.

Therefore, Presidential Decree No. 63 year 2004 concerning national vital objects must be reviewed, including a security model to deal with cyber threats against all vital objects and objects that have not been categorized as vital obedience but have fulfilled these categories. At least the government must determine 11 critical infrastructure, including the Defense and Security Sector, Government Sector, Transportation Sector, Financial Services Sector, Health Sector, Technology, Information & Communication Sector, Energy Sector, Water Sector, Defense Industry Sector, Manufacturing Sector, Food & Agriculture Sector.

CONCLUSION

The Interconnection of information and communication technology infrastructure networks, both civil and military, makes the security of vital national infrastructure increasingly vulnerable. The government must immediately improve policies on national vital objects that still use conventional approaches in understanding modern threats. By establishing a national vital infrastructure, efforts to protect national interests and sovereignty of Indonesia in the cyber domain with a combination approach of strict liability and consequence based approach can be carried out. In

[42] EU Commission, 2008. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union.

addition, cyber attacks in Indonesia can be handled effectively and efficiently by the appropriate and authorized institutions.

REFERENCES

Books:

Budget of the United States Government, Fiscal Year 2017

Blakely, B. A. (2012). Cyberprints: identifying cyber attackers by feature analysis.

Carter, A., 2015. The Department of Defense cyber strategy. The US Department of Defense, Washington, DC.

Carter, A., 2015. The DOD cyber strategy. April, 17, p.2015.

Chen, T.M., 2013. An assessment of the department of defense strategy for operating in cyberspace. Army War College Carlisle Barracks Pa Strategic Studies Institute.

Christopher D. DeLuca, he Need for International Laws of War to Include Cyber Atacks Involving State and Non-State Actors, 3 Pace Int'l L. Rev. Online Companion 278 (2013).

Gheorghe, A. V., Tatar, U., & Gokce, Y. (Eds.). (2017). Strategic Cyber Defense: A Multidisciplinary Perspective (Vol. 48). IOS Press.

Schmitt, Michael N., Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.

Schreier, F., 2015. On cyberwarfare. Geneva Centre for the Democratic Control of Armed Forces.

Tabansky, L., 2011. Critical Infrastructure Protection against cyber threats. Military and Strategic Affairs, 3(2), p.2.

U.K. Government. "National Cyber Security Strategy 2016-2021"

International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, DC: The White House, May 2011)

Janczewski, L. J., & Caelli, W. (2016). Cyber Conflicts and Small States. Routledge.

Jansson Holmberg, E. (2015). Armed attacks in cyberspace: do they exist and can they trigger the right to self-defence?.

K. Saalbach, Cyber War; Methods and Practice. Version 6.0-2 January 2013;1-54.

Kolonel (AU) Rudy Gultom, 2015, Legitimasi Badan Cyber Nasional (BCN) Sebagai Pusat Komando Dan Kendali Kerjasama Antar Instansi Di Indonesia Guna Menghadapi Tantangan Cyberspace Dan Cybersecurity Dalam Rangka Melindungi Kepentingan Dan Ketahanan Nasional, National Cybersecurity Symposium.

Langevin, J.R., McCaul, M.T., Charney, S. and Raduege, H., 2008. Securing cyberspace for the 44th presidency. Center for Strategic And International Studies Washington DC.

Lindsay, J.R., 2013. Stuxnet and the limits of cyber warfare. Security Studies, 22(3), pp.365-404.

Lior Tabansky. Basic Concept in Cyberwarfare.Military and Strategic Affairs.Vol 3. No 1. May 2011. Pg 75-92.

Michael Holloway. Stuxnet Worm Attack on Iranian Nuclear Facilities.Submitted as coursework for PH241, Stanford University, Winter 2015

Muhammad Saleem & Jawad Hassan, "cyber warfare"the truth the real case, Project Report for Information Security Course, Linköping Universitetet, Sweden

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. California Law Review, 817-885.

Richardson, J., 2011. Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. J. Marshall J. Computer & Info. L., 29, p.1.

Jason Porterfield, 2011.Careers as a Cyberterrorism Expert. The Rosen Publishing Group,

Jon Schiller, 2010. Cyber Attacks & Protection: Civilization Depends on Internet & Email, CreateSpace.

Walters, R., 2014. Cyber attacks on US companies in 2014. Heritage Foundation Issue Brief, 4289.

Dissertation

Kazinec, D., 2011. Issues of cyber warfare in international law (Doctoral dissertation, Mykolas Romeris University).

Setiyawan, A. 2018. Penguatan Kebijakan dan Kelembagaan National Cyber Defense dalam Menghadapi Ancaman Cyberwarfare di Indonesia (Doctoral dissertation, Sebelas Maret University).

Internet Sources :

Steve Morgan. 2017. *2017 Cybercrime Report*. Https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf. Accessed 23 September 2018

Ponemon Institute. 2017. *2017 Cost of Cybercrime Study*. Https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf . Accessed 23 September 2018

Achmad Rouzni Noor. 2015. Kerugian Akibat Kejahatan Cyber Tembus USD 150 Miliar. Https://inet.detik.com/security/d-3081840/kerugian-akibat-kejahatan-cyber-tembus-usd-150-miliar. Accessed 23 September 2018

Fauzan Jamaludin. 2016. *Ini jumlah kerugian finansial korban kejahatan cyber.* Https://www.merdeka.com/teknologi/ini-jumlah-kerugian-finansial-korban-kejahatan-cyber.html. Accessed 23 September 2018

Alex Middleton. 2016. *Stuxnet: The World's First Cyber... Boomerang?*. Http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang. Accessed 23 September 2018

Nick Whigham. 2016. *Alex Gibney film gives chilling insight into the world of state sponsored cyber warfare unleashed by Stuxnet*. http://www.news.com.au/technology/online/security/alex-gibney-film-gives-chilling-insight-into-the-world-of-state-sponsored-cyber-warfare-unleashed-by-stuxnet/news-story/a7063ae03dcb5cd6ed2a576d6a8ea9dc, Accessed 23 September 2018

David Kushner. 2013. *The Real Story of Stuxnet*. Http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. Accessed 23 September 2018

Anon. 2010. *Apa itu Stuxnet?*. Http://www.antaranews.com/berita/222505/apa-itu-stuxnet. Accessed 23 September 2018

Anon. 2012. *Virus Flame Diciptakan Untuk Serang Iran*. Http://www.beritasatu.com/iptek/50900-virus-flame-diciptakan-untuk-serang-iran.html. Accessed 23 September 2018

Ellen Nakashima. 2014. *U.S. attributes cyber attack on Sony to North Korea.* Https://www.washingtonpost.com/world/national-security/us-attributes-sony-attack-to-north-korea/2014/12/19/fc3aec60-8790-11e4-a702-fa31ff4ae98e_story.html?utm_term=. Accessed 23 September 2018

Alec Russell. 2004. *CIA plot led to huge blast in Siberian gas pipeline*. Http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1455559/CIA-plot-led-to-huge-blast-in-Siberian-gas-pipeline.html. Accessed 23 September 2018

U.S. Navy. N.d. computer attack. http://www.history.navy.mil/library/online/computerattack.htm Accessed 23 September 2018

HM Government. 2016. *National Cybersecurity Strategy 2016-2021*. Https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national_cyber_security_strategy_2016.pdf. Accessed 23 September 2018

National Audit Office. 2014. *Update on the National Cyber Security Programme*. Https://www.nao.org.uk/wp-content/uploads/2015/09/Update-on-the-National-Cyber-Security-Programme.pdf. Accessed 23 September 2018

National Audit Office. 2014. *Short Guide to the Cabinet Office*. Https://www.nao.org.uk/wp-content/uploads/2017/09/Short-Guide-to-the-Cabinet-Office.pdf. Accessed 23 September 2018

UK Government. 2013. *New cyber reserve unit created*. Https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit. Accessed 23 September 2018

U.S. Government. 2016. *Budget of the US Government*. Https://www.gpo.gov/fdsys/pkg/BUDGET-2017-BUD/pdf/BUDGET-2017-BUD.pdf. Accessed 23 September 2018

Elisabeth Rosenthal & David E. Sanger. 2001. *U.S. Plane In China After It Collides With Chinese Jet*. Http://www.nytimes.com/2001/04/02/world/us-plane-in-china-after-it-collides-with-chinese-jet.html?pagewanted=all. Accessed 23 September 2018

John Goetz and Marcel Rosenbach. 2009. *'Ghostnet' and the New World of Espionage*. Http://www.spiegel.de/international/world/cyber-spies-ghostnet-and-the-new-world-of-espionage-a-618478.html, . Accessed 23 September 2018

Matt Loney. 2004. US *software 'blew up Russian gas pipeline'*. Http://www.zdnet.com/us-software-blew-up-russian-gas-pipeline-3039147917/. Accessed 23 September 2018

Ministry of Communication and Multimedia Malaysia. n.d. https://cnii.cybersecurity.my/main/about.html Accessed 23 September 2018

UK Government. N.d. Https://www.gov.uk/government/organisations/joint-forces-command/about/recruitment Accessed 24 August 2018

Annon. 2010. War in the fifth domain. http://www.economist.com/node/16478792, Accessed 23 September 2018

Department of Homeland Security. N.d. https://www.dhs.gov/office-infrastructure-protection Accessed 24 September 2018

Michael B Kelley. 2013. The Stuxnet Attack On Iran's Nuclear Plant Was 'Far More Dangerous' Than Previously Thought. http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11?IR=T&r=US&IR=T. Accessed 23 September 2018

Anthony Wood. 2014. South Korea pushes for cyber weapon to undermine North Korean nuclear facilities. http://newatlas.com/south-korea-stuxnet-cyber-weapon/30977/ Accessed 23 September 2018

Kim Zetter. 2014. An Unprecedented Look at Stuxnet, the World's First Digital Weapon. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ Accessed 23 September 2018

Rachel Williams Global hackers threaten net security in cyber warfare aimed at top targets. http://www.theguardian.com/technology/2007/nov/29/hacking.news.Accessed 23 September 2018

Rachel William. 2007. *Global hackers threaten net security in cyber warfare aimed at top targets*. Http://www.theguardian.com/technology/2007/nov/29/hacking.news. Accessed 23 September 2018

Legislation:

Presidential DecreeNo 63 tahun 2004 Tentang Pengamanan Objek Vital Nasional

Obama, B., 2013. Presidential policy directive 21: Critical infrastructure security and resilience. *Washington, DC*.

EU Commission, 2008. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Official Journal of the European Union.

Presidential Decission Directives/PPD-63 Year 1998

H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001