STRENGTENING INDONESIA'S POLICY ON NATIONAL CYBER SECURITY TO DEAL WITH CYBERWARFARE THREAT

Anang Setiyawan
Jamal Wiwoho
Rahayu

ABSTRACT

In 2012 IACSIRT recorded thousands of cyber-attacks against the Indonesian domain and millions cyber attacks over the past few years. In 2009 the Indonesian Embassy and Foreign Affairs Office became one of the targets of the Ghost Net virus which is a large-scale espionage operation conducted by China and in 2010 the industrial sector in Indonesia has been one of the targets of the powerful Cyber Stunext virus series attacks. The Stunext virus is the most sophisticated and dangerous cyber weapon ever made. if the attacks were directed to vital infrastructure such as electric power sources, mass transportation, air traffic control systems or even nuclear power plants that would not only cause malfunctions, wounds and deaths. The results of this study are as follows; (a) Cyberwarfare is subject to International Humanitarian Law Principles, (b) Strengthening policies on national cyber defense is necessary and the government needs to strengthen the policy by formulating an act as legal basis, so that these complex and multi-domain issues can be handled comprehensively. Moreover cyber-attacks can be used systematically, effectively to weaken defense systems, security, sovereignty, economy and politics of a country

Key words: cyberwarfare, strengthening, Indonesia, sovereignty, national interest

Introduction

Military strategies and weapons of a country can reflect economic, political conditions and describe the supremacy and ability to technology[1]. The technology development shifts the social concept in society[2] and the conventional war that are physically-kinetic in the domain of land, sea, air, space to the modern war by non-kinetic weapons in the fifth domain called cyberspace[3]. The cyberwarfare emphasizes attacks through computer networks that aim to cause certain expected damage or dysfunction with certain political or national security motives without crossing a country's boundaries[4]. Currently, cyber capability is the heart and new war doctrine based on modern technology and makes it as the most influential instrument in all levels of conflict because it able to provide new techniques to increase speed, scale and attack power[5]. The British House of Commons Defense Committee stated that the cyber threat is, like some other emerging threats, one which has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation's security[6]. Although cyber attacks are carried out from computers but these attacks can lead to disruptions and destruction of networks of civil and military infrastructure that are very difficult to limit and predict its impact and size. Cyber attacks are successful not only measured by the consequences of physical destruction, but also on their influence on the economic stability of a country and basic services to civil society such as water, electricity, communications, transportation, emergency services, etc.

Several cases that have occurred before, such as the Russian cyber attacks against Estonia (2007) that almost caused the economic paralysis due to the high dependence on information technology infrastructure in all areas[7]. CIA's Cyber Attacks against gas pumps and valves led to out of control and consequently Soviet gas pipelines in the Siberian region exploding and recorded as the biggest explosion ever seen in addition to nuclear bomb explosions[8]. US and NATO cyber attacks to disable and deceive the Serbian Air Defense and Serbian Air Traffic Controller. This attack also blocked Yugoslavia's communications

[1]Smits, T. V. (2000). *Computer Network Attack As a Tool for the Operational Commander*. Naval War Coll Newport RI Joint Military Operations Dept.
[2] Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loy. LA Int'l & Comp. L. Rev.*, *32*, 303.
Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825-865.
[3] http://www.*economist*.com/node/16478792 accessed January 2013
Melzer, N. (2011). *Cyberwarfare and international law*. United Nations Institute for Disarmament Research.
[4] 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.
[5] Schreier, F. (2015). *On cyberwarfare*. Geneva Centre for the Democratic Control of Armed Forces.
[6] House of Commons Defence Select Committee. (2012). Defence and Cyber-Security. *Sixth Report of Session*, *13*, 11.
[7] Saleem, M., & Hassan, J. (2009). " Cyber warfare", the truth in a real case. *Project Report for Information Security Course, Linköping Universitetet, Sweden*.
http://www.theguardian.com/technology/2007/nov/29/hacking.news accessed January 2013
[8] 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 January 2013

network during the conflict[9]. The similar strategy was applied by the Israeli air force when attacking a nuclear facility in Syria without detected by an air defense radar system in September 2007[10]. Operation Moon Maze (1998-2000) is allegedly carried out by Russia to dig data in Pentagon computer systems, NASA and the Department of Energy America that caused 10,000 important files lost. In 2009, China was also suspected of carrying out a large-scale, systematic cyber attack known as GhostNet and Aurora Operation. GhostNet is a cyber attack using viruses against several embassies including India, South Korea, Indonesia, Taiwan, Thailand, Pakistan and Germany. This attack also attacked the Foreign Ministry of Indonesia, Iran, Bhutan, Bangladesh, Brunei. The virus has the ability to activate and control the webcam, an infected computer microphone. Operation Aurora is used to access computer programs, source code from the information technology sector, security and defense companies. US and Israeli cyber attacks on Iran's Uranium enrichment program via the Stunext[11] virus in 2010 and attacked the Iranian and Middle East government offices through the Flame virus in 2012 that could enable to activate equipment connected to computer networks and communications[12].

The cases demonstrate how cyberattacks can be used systematically to weaken and disrupt defense systems, economic systems, public infrastructure systems and other vital infrastructure networks related to the safety and security of a country. Unlike conventional wars that are easier to enforce the Principles of International Humanitarian Law (IHL) but not so in cyberwarfare. The application of International Humanitarian Laws and Principles in the context of Cyberwarfare has some fundamental issues, i.e. this domain can be created, owned operated collectively from around the world, techniques and methods of war that are elusive except by the experts, the anonymity of the attacks, interconnection of civil and military computer networks, the absence of any implicit international legal or customary is also a problem as the parties can define the provisions and principles of international humanitarian law in accordance with the interests of their respective countries[13].

The lack of the IHL provision that implicitly impose on cyberwarfare does not mean that the hostile parties can override humanitarian values as the understanding of the International Humanitarian Law and Principles is not limited at that time. ICRC Legal Adviser stated that "*All IHL rules governing the conduct of hostilities are potentially applicable during armed conflict….that one of the main purposes of IHL is to protect the civilian population and civilian infrastructure from the effects of hostilities*"[14]. Eugene Kapersky stated that the global cyber war will more dangerous and escalate every year[15]. The attack will be more systematic and sophisticated than ever and the dependence on information technology is directly proportional to the potential risks and threats to the national interests of a country. Currently, some developed countries including America, China, Russia, Israel, Italy and Germany have stated cyberspace as new war domain, formulating national cyber defense policies and forming cyber units prepared to equip their military forces to carry out attacks while defending against attacks in cyberspace since the last decade.

Indonesia with more than 132.7 million internet users[16] connected with more than 4 billion internet users worldwide[17] provide more attention to cyber security because in 2012 Indonesia Academic Computer Security Incident Response recorded 8055 cyber attacks against Indonesia[18] and total more than 3.9 Million cyber attacks over the past 3 years[19]. In 2009 the Indonesian Embassy and Foreign Affairs Office became one of the targets of the GhostNet virus which is a large-scale espionage operation conducted by China and even in 2010 the industrial sectors in Indonesia became one of the targets of the stunext virus which is considered the most sophisticated and dangerous cyberweapon ever made[20]. If the attack was intentionally directed to power plants, dam systems, air traffic control systems, defense systems, public transport systems, banking systems or even nuclear power plants will not only cause malfunctions but potentially cause physical damage, injuries and even death to civilians[21].

---

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

[10] 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.

[11] Discovered in June 2010 and referred to "the world's first fully fledged cyber weapon" created by the United States and Israel as part of a joint operation called the "Olympic Games" operation. In the context of cyberwar Malware is referred to as a "game changer", unlike the nature of cyber attacks against Estonia and Georgia using DDOS techniques, this malware has a target and is designed with very sophisticated to destroy certain physical targets. Stunext can cause malfunctions on nuclear enrichment until it can self-destroy automatically. http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang

[12] 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/, accessed January 2013

[13]http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm accessed February 2013
Kellenberger, J., & Spoerri, P. (2012). International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011.

[14] Droege, C. (2011). No legal vacuum in cyber space. *ICRC, Interview*, *16*.

[15] http://rt.com/news/mini-flame-malware-kaspersky-519/ accessed January 2013

[16] http://www.internetworldstats.com/asia.htm#id accesed January 2018

[17]http://www.internetworldstats.com/stats.htm accessed January 2018

[18]http://inet.detik.com/read/2012/01/20/105656/1820779/323/7-negara-asean-yang-paling-sering-kena-serangan-web/). accessed Januari 2013

[19]Zainal A. Hasibuan, *Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace*. Dewan Teknologi Informasi dan komunikasi Nasional. 2013. http://www.merdeka.com/teknologi/hacker-china-incar-militer-negara-negara-asia-indonesia-termasuk.html accessed January 2013

[20] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, *22*(3), 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/, http://teknologi.news.viva.co.id/news/read/166993-trojan-scada-hantui-iran-indonesia-india accessed January 2013

[21] http://www.thefiscaltimes.com/Articles/2013/03/11/The-Coming-Cyber-Attack-that-Could-Ruin-Your-Life accessed January 2013

The Ministry of Defense in 2013 began to formulate policies, prepare technical capabilities, formulate a national cyber defense strategy strategy and establish cyber units. This unit will ward off attacks that disrupt Indonesia's national sovereignty, defense, security and national interests[22]. In 2015 the government issued Presidential Regulation no. 97 of 2015 concerning general defense policy of state. The principal of defense policy related to the handling of cyber threats only regulates the development of technology and information systems and communication which is directed to improve the quality of state defense information system. This policy only improves the quality of infrastructure and technology in facing cyber threat while the national cyber defense policy comprehensively is unclear. From the description above, the authors want to study application of international humanitarian law principles in the cyber domain and how Indonesia strengthens the National Cyber Defense policy in order to deal with cyberwarfare threat while maintaining the defense, security and national interests of the Indonesian state in the real and cyber domain.

Discussion

1. Application of International Humanitarian Law Principles on Cyber Domains

The principles of IHL apply not only to conventional wars but also to cyberwarfare. This is important to examine as it relates to the enforcement of basic provisions of IHL during conflicts such as precaution, civilian protection, prohibition of indiscriminate attack, etc. The principle of humanitarian law can be applied to cyberwarfare with several legal basis. First, a cyber attack can be defined as an attack intended in Article 49 (1) of Additional Protocol I. Some experts, Bothe, Partsch, Solf stated that 'acts of violence' in this Protocol refers to physical force, therefore attacks carried out with computer networks that cause physical injury or damage to objects can be defined as attacks in IHL[23]. ICRC provides a broader understanding, asserting that attack that disable an objeck can be categorized as an attack even though the attack does not cause physical injury, death or damage[24]. Therefore according to Article 2 of the 1949 Geneva Convention, IHL may apply to cyberwarfare. Second, the Marten Clause as a principle of humanitarian law ensures that no action in armed conflict is not governed by IHL and the fundamental limits of IHL remain in force. Under this clause all armed conflicts are subject to the application of the principles of IHL. Third, the International Court of Justce (ICJ) on its advisory opinion on nuclear weapons rejects the claim that humanitarian law cannot be applied because the "*rules and rules have evolved prior to the invention of nuclear weapons*" in this case the ICJ argues that "*in the view of the vast majority of States as well as the applicants of humanitarian law to nuclear weapons*". So it can be concluded that the principles of IHL can be applied to cyberweapon on cyberwarfare as well as the use of nuclear technology in conventional warfare. In addition, the ICJ argues that in this advisory opinion there are two fundamental legal restrictions that apply to weapons. First, the prohibition to make civilian as military objectives and therefore prohibit the use of weapons that cannot distinguish the objective. Second, the prohibition to cause unnecessary suffering to the enemy, therefore it is prohibited to use weapons that can cause excessive suffering. According to the ICJ, this clause is an effective tool for dealing with the rapid development of weapons technology by keeping these values in it.

a) Distinction Principle

The principle of this distinction is one of the main principles of humanitarian law as stated in the advisory opinion of ICJ on nuclear weapon of 1996[25]. The principle of distinction can be found in several instruments of IHL, including the Hague Convention 1907, Geneva Convention 1949, Additional Protocol I 1977. Under Article 48 Additional Protocol I that parties must always distinguish between civilians and combatants as well as civil and military objects civilians and civilian objects should not be targeted. It even prohibits attacks on objects that are indispensable for the survival of civilians such as food and beverage supplies as set forth in Article 54 (2) Additional Protocol I.

In the context of cyber attacks, it is necessary to extend protection to civilians and civilian objects that may be affected indirectly due to the connectivity of civil and military networks. Cyber attacks directed at military targets may be widespread and affect the civilian information system and communication network. Cyber attacks committed against all enemy computers and networks without distinguishing properties, usage, purpose and location can be categorized as indiscriminate attacks. Such an attack is similar to Iraqi attack on the Saudi Arabian and Israeli population centers using a Scud missile at the Gulf War 1991. This weapon basically a high accuracy weapon and not classified as "*indiscriminate weapon*". But using a missile to attack targets at the population center is considered an indiscriminate attack even though the attack is directed at a military object because the impact of the attack causes more civilian casualties than a legitimate objective. The case is similar to the 2007 Martic case, where the ICTY stated that firing unmanned rockets with clusters bullet from the maximum distance range to the heavily populated city of Zagreb was an indiscriminate attack due to bullets dispersion when fired from a maximum distance[26].

b) Proportionality Principle

[22] http://www.antaranews.com/berita/399394/cyber-army-antisipasi-cyber-warfare accessed Januari 2013

[23] Dörmann, K. (2004, November). Applicability of the Additional Protocols to computer network attacks. In *International Expert Conference on Computer Network Attacks and the Applicability of IHL, Stockholm* (p. 3).

[24] Schmitt, M. (2012). Classification of cyber conflict. *Journal of conflict and security law*, *17*(2), 245-260.

[25] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996

[26] Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. *Journal of Conflict and Security Law*, *17*(2), 261-277.

The proportionality principle governs a situation that endangers protected civilians or civilian objects from the consequences of attacks on the intended targets but that is not a stated goal. This principle is most often violated as a result of a lack of sufficient understanding of the object, due to the inability to know the amount of force directed to the target and the inability to ascertain the accuracy of the weapons used against the intended target. Basically, these issues can be minimized in the context of an attack through a computer network.

Article 51 of Additional Protocol I states that an attack is considered as an indiscriminate attack and violates proportional principle if "*may be expected to cause incidental loss of civilian life, or a combination thereof, which would be excessive*..". Thus Article 57 (2 (a) (iii)) requires the parties to "*...refrain from deciding to launch an attack which may be expected to cause incidental ...*" *(but) excessive (losses) ... in relation to the concrete and direct military advantage anticipated*...". Even according to Article 57 (2 (b)) the attack shall be abrogated if "*...if it be apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive...*". Article 8 (2) (b) (iv) Rome statute affirms that "*...extensive destructions...not justified by military necessity...or damage... and direct overall military advantage anticipated*..." [27]. Regarding this principle, the ICRC declares that "*Launching an attack which maybe expected to cause incidental loss of civilian life, injury to civilian, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, is prohibited.* "*Excessive*" itself is described as "*…disproportion between losses and damages caused and the military advantages anticipated rasies a delicate problem; in some situations there will no be no room for doubt, while in other situations there may be reason for hesitation. In such situation the interest of the civilian populations should prevail*".[28]

The calculated military advantage is generated from the overall operation. The proportionality principle requires a balance between military advantage and the impact of the attack. This becomes difficult because the military advantage resulting from an attack depends on the parties at that time. Placing that principle in practice is recognized very difficult, the additional protocol I explain that "*putting these provisions into practice… will require complete good faith on the part of the belligerents, as well as the desire to conform with the general principle of respect for the civilian population*". To decide to use cyber weapons commanders are required to perform in-depth analysis as well as when to conduct an attack with a conventional kinetic weapon[29].

A complex problem that arises later is what is called a "*knock-on effect*" or "*unexpected consequence*", namely "*known as second and third tier effects that were not accounted for in the planning stages of the attack, but occur due to some unexpected agent or circumstance*"[30]. This term can simply be defined as a series of indirect impacts caused by cyber attacks. As cyber attacks on the power grid in Iraq at the Gulf war, although considered successful in disrupting Iraqi control and command, but also affects hospital service, emergency response, etc. The impact of "*Knock on Effect*" not only resulted in physical damage but could be in other wider forms such as the Nigerian rebel's "MEND" cyber attacks against oil companies in 2006, though it did not cause disruption to oil refinery operations but making the oil market tense and causing oil prices to rise. Knock on effect on cyber attacks has the potential for greater impact than kinetic attacks due to the interconnectivity between military and civilian network systems. The complexity of cyber attacks enables a large impact on the civilian system and therefore the hostile party should be able to assess the potential impacts of damage and injury that may arise during the planning process of the attack. Therefore, modeling and simulating attacks as well as the use of nuclear weapons will be essential in order to identify potential knock-on effects and reduce possible collateral damage. Such as the sophistication of the "*stunext*" weapon that infects only certain network objectives so as to minimize the impacts[31]. James A. Lewis name it "*Battle Damage Assessment*" which aims to measure the impact of cyber attacks so that the attacks are more effective, precise and able to minimize the impact of attacks on civilians and civilian objects in accordance with IHL[32].

2. National Cyber Defense Policy in Indonesia

a. National Cyber Defense Policy Development Issues in Indonesia

The Indonesian government is currently at the stage of policy formulation, information system security and defense strategies in order to deal with cyber threats. Based on an analysis of environmental developments and the strategic context of threat estimates, challenges and risks of state defense, the Ministry of Defense determined that the defense policy of both military

[27] Gervais, M. (2012). Cyber attacks and the laws of war. *Berkeley J. Int'l L.*, *30*, 525.
https://www.icc-cpi.int/resourcelibrary/official-journal/elements-of-crimes.aspx#article8-2a-iv Accessed 29 Juli 2017
[28] Casey-Maslen, S. (Ed.). (2014). *Weapons under international human rights law*. Cambridge University Press.
[29] http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2015_Ch9.pdf
https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/b466ed681ddfcfd241256739003e6368/d80d14d84bf36b92c12563cd00434fbd accessed August 2017
Melander, G. (2006). *Essays in Honour of Göran Melander* (Vol. 26). Martinus Nijhoff Publishers.
Rogers, A. P. V. (2013). *Law on the Battlefield*. Oxford University Press.
Martin, F. F., Schnably, S. J., Wilson, R., Simon, J., & Tushnet, M. (2006). *International human rights and humanitarian law: treaties, cases, and analysis*. Cambridge University Press.
[30] Jensen, E. T. (2002). Unexpected consequences from knock-on effects: a different standard for computer network operations. *Am. U. Int'l L. Rev.*, *18*, 1145.
[31] Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365-399.
Richardson, J. (2011). Stuxnet as cyberwarfare: applying the law of war to the virtual battlefield. *J. Marshall J. Computer & Info. L.*, *29*, 1.
[32] Lewis, J. A. (2013). *Conflict and negotiation in cyberspace*. Washington, DC: Center for Strategic and International Studies.

defense and non-military defense would have cyberdefense capability[33]. According to the government, the development of conventional weapon technology innovation is still growing but the development of science and technology greatly affect the shape and pattern of war in the future one of them create a war-based network of information and communication technology. The base of this war has significantly altered strategic security especially with the use of communication and information networks across sectors, especially in the defense sector.

Indonesia's efforts in realizing and developing the cyber capabilities will face several challenges such as inadequate cyber-policy and regulatory arrangements, weak coordination and cooperation between government and private sector, governance of cyber security and related national organizations are lack of synergy, lack of standards and mechanisms protection of vital infrastructure, not integrated vital information infrastructure, limited quality and quantity of human resources in the cyber security sector[34]. The fundamental problem related to cyber attacks in Indonesia is the use of narrow perspectives in understanding cyber threat. Cyber attacks are only considered as a crime and under the Indonesian police domain. This is understandable because the legal issues related to infringement, crime and cyber security in Indonesia are covered by limited legal rule. Some rules related to cyber domains and threats through cyber domains, as follows:

1) Criminal Code (KUHP)

Basically KUHP is not specifically designed to deal with crimes committed in the cyber domain but some articles in the Criminal Code can be used to ensnare certain types of crimes committed in this domain by using extensive interpretation. Some criminal cases in Indonesia that use this interpretation such as the case of electricity theft which extends the interpretation of the word "goods" in article 362 of the Criminal Code not only on "tangible goods" but also "intangible goods"[35]. This extensive interpretation is used in some articles in the Criminal Code related to crimes committed in the cyber domain, including article 282 which can be used to ensnare pornographic cases through internet media, article 311 that can be used to ensnare defamation cases through internet media, sections 362 and 378 which can be used for cases of credit card number theft and article 303 that can be used to ensnare online gambling cases.

2) Act No. 11 Year 2008 on Information dan Electronic Transaction.

Basically, this Law regulates the problem of cybercrime, ecommerce, Haki protection, consumer protection and unfair competition. Criminal provisions in this Law are contained in Chapter XI Section 45-52 on Criminal provisions, some prohibited acts related to information technology crime, such as Article 30 are used to ensnare criminal access, intercept, break into computer systems or electronic systems illegaly. Article 31 is used to ensnare criminal acts of interception of electronic information and or electronic systems in a particular computer and or other electronic system. Article 32 is used to ensnare a criminal act of destructive transmission, removal, transfer, concealment of electronic information and or electronic documents and or electronic documents. Article 33 is used to ensnare criminal acts of illegal conduct resulting in disruption of electronic systems being unable. Article 34 is used to ensnare the criminal act of producing, selling, organizing for use, importing, providing computer software for the purposes of decency or sexual exploitation of children, tapping, destroying and removing electronic information and or electronic documents and / or electronic documents of persons other or public property. And Article 35 is used to ensnare a crime of alteration, creation, destruction, disappearance and manipulation of electronic information data / electronic documents with the purpose of electronic information and or documents considered as authentic data.

3) Act No 36 year 1999 on Telecomunication

The provisions related to the information technology crime in this Law are as follows (a) Article 21 states that telecommunication operators are prohibited from conducting business activities of telecommunications that are contrary to public interest, morals, security, or public order. This Article excludes crimes and is not subject to criminal provisions. The provision against this is only an offense under Article 46 of its sanction in the form of revocation of permit, (b) Article 50 regulates unlawful acts or manipulates access to special telecommunication networks, (c) Article 55 regulates acts that may cause electromagnetic physical damage to telecommunication providers, and (d) Article 56 prohibits anyone from intercepting information transmitted through telecommunication networks of any kind. Elucidation of Article 40 states that wiretapping in this article is the activity of installing any equipment or enhancements in the telecommunication network for the purpose of obtaining information illegally.

4) Ministry of Defense Decree No. KEP/435/M/V/2016 on State Defense Policy year 2017

The State Defense Policy is organized with a universal defense system through development of resources, national infrastructure and the entire territory of the unitary state of the Indonesian republic as a single unit of defense in the face of threats. This defense policy divides the threat into two types, namely military threat and nirmiliter threat. The military threat faced by the military defense system by placing the Indonesian National Army as the main component supported by the reserve components

[33] Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia.
[34]Zainal A. Hasibuan, Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace. Dewan Teknologi Informasi dan komunikasi Nasional. 2013
[35] http://www.hukumonline.com/berita/baca/lt559fba87c3065/putusan-ibonda-i-yang-mengayun-bismar
Accessed November 2017
Christianto, H. (2010). Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana. *Pamator Journal*, *3*(2), 101-113.

and supporting components. While nirmiliter threat faced by nirmiliter defense system by placing the institution of government outside the field of defense as a major element in accordance with the form and nature of the threat faced with the support of other elements of the power of the nation. This policy is formulated by considering the dynamics of the strategic environment that pose threats and impacts on national defense.

The defense policy has a vision of the state defense development that is "the realization of a sovereign, independent and person-based Indonesia based on mutual cooperation". This vision is manifested through seven defense development mission, including; (a) Realizing national security capable of maintaining regional sovereignty, sustaining economic independence by securing maritime resources, and reflecting the personality of Indonesia as an archipelagic country. (b) Creating an advanced, balanced, and democratic society based on the rule of law (c) Realizing a free-active foreign policy and strengthening identity as a maritime country (d) Realizing the quality of human life of Indonesia, (e) Creating a competitive nation, (f) Making Indonesia a maritime state that is independent, advanced, strong, and based on national interests and (g) Realizing a society of personality in culture.

To realize the government's vision, mission and agenda of priorities on the development of state defense, the defense ministry formulates strategic objectives, as follows; (a) Realizing the country's defense capability to deal with threats, (b) Creating th country's defense capability to deal with the security of maritime, the mainland and the aerospace, (c) Creating a strong defense industry, independent and competitive, and (d) Creating country defense awareness for Indonesian citizens. One of the main policies of state defense is the development of information technology and defense communications. The development is carried out by integrating state defense information systems using satellites, optimizing cyber defense in accordance with cyber defense guidelines, encouraging relevant ministries and agencies to master defense technology in producing defense equipment, encouraging related ministries and agencies in human resource development and technological information and communication infrastructure development.

The Cyber Defense Guidelines set forth in Ministry of Defense Regulation No. 82 Year 2014 on the Guidelines of Cyber Defense is the basic reference for ministry of defense and Indonesian Army to organize cyber defense. The cyber defense guideline is the embodiment of determination, principle and will to organize cyber defense in information systems, controls and communications in the defense sector. This guideline embodies a framework for the organization of cyber defense that must be implemented in accordance with their respective duties and functions. Cyber defense is a nirmiliter defense force that makes the Ministry of Communications and Information as the main element and the defense ministry as supporting elements. Making the concept of cyber defense as a part of nirmiliter defense describes a lack of understanding of the impact of cyber threats that multispectrum and complex. The government should more concern to the target, the attack level, the attack scale and its impact in determining the concept of defense. The absence of a common policy between all ministries and agencies in understanding the cyber threats has made every ministry and agency deal with cyber threats run partially and sectorally.

This cyber defense guideline policy concern to the sectors that manage critical infrastructure in the areas of defense, security, energy, transportation, financial systems and other public services. The disruption to the sector can have an impact on the economy and a decrease in the level of trust in government and public order. However, these sectors have not been defined, described and the government needs to appoint a leading sector as the coordinator of each sector. In addition, the government needs to harmonize the policy of determining this vital infrastructure with the policy on the national vital object which is regulated in Presidential Decree no. 63 Year 2004.

Limitations of existing rules and the formulation of the above provisions have a limited and sectoral perspective in view of a major threat to the national interests of Indonesia through cyberspace. This field of security and defense is difficult to separate because of the characteristics of cyber attacks that are more complex than the characteristics of crime or other conventional attacks. Therefore, it is needed a policy that can elaborate the two fields into one so that the handling of cases that occur in Indonesia can be completed properly and efficiently. The policy tables related to cyber threats can be described as follows:

Table 1: Taxonomy of Regulations Related to Cyber Threats in Indonesia

Regulation / Threat	*Cyber Crime*	*Cyber Terrorist*	*Cyber Warfare*
Act	- Criminal Code - Information & Electronic Transaction Act - Telecomunication Ac	- Terorism Act - Criminal Code - Information & Electronic Transaction Act - Telecomunication Act	
Presidential Decree & Presidential Regulation			- Presidential Regulation No. 53 Tahun 2017 on BSSN - Presidential Regulation No. 97 Tahun 2015 on General Policy of Defense 2015-2019
Ministry Regulation			- Ministry of Defense decree No: KEP/387/M/IV/2015 on Pembina Sistem Informasi dan Komunikasi pada Sistem Informasi Pertahanan Negara dan Pertahanan

			Siber - Ministry of Defense decree No. KEP/435/M/V/2016 on Defense State Policy Year 2017 - Ministry of Defense regulation No. 82 Year 2014 on Cyber Defense Guidelines - SK Kemenkopolhukam No. 5 year 2015 on DK2ICN

b. Strengthening National Cyber Defense Policy in Indonesia

Government policy on cyber defense is stated in Presidential Regulation No. 97 of 2015 on general policy of state defense 2015-2019. The Presidential Regulation slightly discussed on the development of information and communication technology including the cyber defense development. This policy is the cornerstone for Indonesian cyber defense development although this policy is not elaborated further. The cyber defense policy made before this Presidential Regulation up to now is organized sectorally by several state institutions with lack of coordination and clear direction how to make cyber defense in maintaining security, national interests and sovereignty in cyber domain. Governments in formulating national cyber defense policies should notice the cyberspace domain as a means to achieve national strategic objectives as well as using other domains to achieve national strategic objectives. The cyberspace domain needs to be maintained because of its contribution to essential daily services, national security, trade, innovation, and information, etc[36]. Formulating an ideal cyber defense policy in Indonesia, the government should take into account Liddle's notion that a country's defense capability is affected by its economic level. The economic level affects the ability to finance the State's defense and becomes the decisive factor behind military force. Conversely, military power can be used to influence the economic development of a country[37].

Cyber defense and security policies in countries such as the United States, Estonia and Malaysia show the same pattern that these countries give priority to the security of infrastructure networks in the economic sector because they can be used as a means to improve prosperity as well as being part of the military strategy of their respective countries. These countries make the infrastructure network in the economic sector as one of the vital infrastructure network. In order to develop the cyber defense and security in Indonesia there are some notes that should be noticed and implemented by the government immediately, including:

1) The government should immediately reassess the level of attacks and potential cyber threats to Indonesia's national security and interests.

The assessment aims to see comprehensively and determine the level of cyber threats to Indonesia's vital sectors not limited to the areas of defense and security but the wider national interests of Indonesia, such as sectors that support the Indonesian economy. Through this assessment the government may also determine and mapping out the vital sectors of Indonesia that are potentially affected by cyber attacks so as to enact appropriate defense, security and mitigation strategies to minimize the impact of the attacks.

Indonesia does not use the term vital Infrastructure, but uses the term national vital object. Presidential Decree 63 Year 2004 defines national vital object as area/location, building/installation and or business concerning the livelihood of many people, state interest and or strategic source of state income. The national vital objects are those that produces basic daily necessities; threats and disruptions to them result in disasters against humanity and development; threats and disruptions to it result in national transport and communications chaos; and/or threats and disruptions to it result in disruption of state administration. The definition is limited; the point of view is tangible although the categorization of vital national objects is broad. This affects how the model of security and the response of government organs in the event of a cyber attack on the national vital object. Infrastructure is said to be vital if it's disruption can cause significant socio economic crises and the potential to undermine the stability of a society, causing political, strategic and security impacts. There are three factors that can be used to define vital infrastructure, namely[38]; a) The symbolic importance of the infrastructure, including cultural heritage sites, museums, archives and monuments as critical infrastructure that must be protected, b) The immediate dependence on infrastructure. These dependencies such as dependence on electricity networks and communications networks are widely used by the community, c) The complex dependencies. The tendency to accelerate the ability of connectivity enables the emergence of unanticipated effects. The interconnection between the various infrastructures is not fully known and the failure of one component can cause extensive impact and damage.

By comparison, United States define vital infrastructure as *"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private"*[39]. Term *'critical infrastructure'* also interpreted as *systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security,*

[36] Wamala, F. (2011). ITU National Cyber Security Strategy Guide. *International Telecommunications Union*, *11*.
[37] Bakrie, C. R. (2007). *Pertahanan negara dan postur TNI ideal*. Yayasan Obor Indonesia.
[38] Types of failure are divided into 3 categories, ie; (1) Common cause failure (2) Cascading failure and (3) Tabansky, L. (2011). Critical Infrastructure Protection against cyber threats. *Military and Strategic Affairs*, *3*(2), 2.
[39] Presidential Decission Directives/PPD-63 Year 1998

national public health or safety, or any combination of those matters"[40]. In PPD-21 2013, America has 16 vital infrastructure sectors which assets, systems, networks both physical and virtual that its inability or damage will have an impact on weakening the national economy, national security, public health or safety or a combination of those impacts[41].

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, health, safety, security, 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 defines as a Critical Infrastructure if a vital infrastructure in a member State which, when disturbed or destroyed, will have a significant impact on at least 2 member states. The significance of these impacts is judged on cross-cutting criteria[42].

From definitions above there are several patterns of similarities used to define critical infrastructures, such that protected objects are not limited to tangible but intangible assets (virtual assets, systems, programs), cyber threats to both are perceived as interfering with national security and interests states, attempts to influence, disrupt and disabling the vital infrastructure system is considered an attack on the state and all sectors categorized as vital objects are objects related to state security, government administration, sustain and support the national economy, the interests of basic people's fulfillment including transportation, health and emergency services services, state strategic industries and information systems organized by those sectors. Therefore Presidential Decree No. 63 of 2004 on the national vital objects must be reviewed as well as the security model in order to deal with cyber threats to all vital objects and objects that have not been categorized obek vital but has met the category.

2) Taking measures and maximize cyber security protection for all assets and infrastructure that considered vital in Indonesia.

This precaution must be implemented immediately because cyber security risks faced by Indonesia is increasing. The large number of attacks increases the risk to Indonesian national security and interest in the cyber domain. These safeguard measures can be implemented immediately by mapping, maximizing and utilizing existing cyber security-related institutions in Indonesia. All these safeguards shall be carried out comprehensively, integrated, structured and under the coordination of the authorized institution.

3) The government should immediately formulate a national cyber defense and security policy.

National defense and security policies include defining a vision, developing regulations, defining national institution dealing with cyber security issues, defining vital assets and infrastructure related to Indonesia's national security and interests, optimizing and encouraging self-reliance in the development of cyber security technologies by state-owned enterprises, optimizing the education to prepare and improve human resources, encourage public awareness about cyber security and interact in cyberspace to conduct research related to cyber security technology. This defense and security policy includes pro-active collaboration and collaboration with various countries and stakeholders related to cyber security. Cooperation with other countries, international organizations related to cyber security can assist law enforcement in case of incidents or cyber attacks[43]. The previous view of a passive defense must move toward the concept of active defense. This defense concept is more active in the detection of various cyber threats at an early stage while allowing taking precautions and even pre-emptive attack on the source of the threat before the threat becomes real[44].

4) The Government should immediately build, strengthen and complement the information and communication technology infrastructure related to Indonesia's national defense and security.

In this context, including, first. Cooperate with universities to develop better cyber security research as well as to encourage the quantity and quality of human resources in the cyber security through education and training. Second, Encourage the autonomy of cyber security technology development and national industry engaged in the information technology and cyber security sector. Third, encourage cooperation with cyber security companies to improve the security of Indonesia's cyber domain.

Conclusion

1. That cyber warfare is subject to the principles of international humanitarian law as well as conventional wars. Principles of International Humanitarian Law can be applied to conventional warfare and cyberwarfare in accordance with the

[40] H.R.3162 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001
[41] Obama, B. (2013). Presidential policy directive 21: Critical infrastructure security and resilience. *Washington, DC*.
[42] To determine the European Critical Infrastructure (ECI) is identified by 3 cross-cutting criteria, i,e. (1) Casualities Criterion; (2) Economic Effect Criterion and (3) Public Effect Criterion. This cross-cutting criteria threshold is based on the level of disturbance and damage experienced by the infrastructure.
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*.
[43] According to the Cisco white paper, to improve the security of the cyber sector as a whole the government should collaborate include with supplier, private Sector, all levels of government organizations and other countries.
http://www.cisco.com/c/dam/en/us/products/collateral/security/security-benchmark-study-government.pdf. accessed 14 agustus 2017
[44] https://ccdcoe.org/cyber-definitions.html accessed Januari 2013

provisions of international Hmaniter Law, Marten Clause and the International Court of Justce (ICJ) on its advisory opinion on nuclear weapons. The potential impact of cyber attacks can be minimized by modeling and simulating attacks that are useful in identifying potential knock-on effects and reducing collateral damages that may arise through an approach known as "Battle Damage Assessment" which aim to measure the impact of cyber attacks so that attacks can be more effective, precise and able to minimize the impact of attacks on civilian and civil objects in accordance with international humanitarian law.

2. Strengthening policies to deal with cyber threats by establishing cyber security policy in the form of act so that it will be easier to facilitate, strengthen and coordinate the handling of various cyber threats that will involve various stakeholders from the government, private sector, other organizations, industry, academic world and research related to cyber security. Without a strong legal foundation will potentially lead to a classic problem of intercultural coordination within it that is linked in an effort to deal with cyber threats.

References

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

Bakrie, C. R. (2007). *Pertahanan negara dan postur TNI ideal*. Yayasan Obor Indonesia.

Buku Putih Pertahanan Indonesia 2014, Kementerian Pertahanan Republik Indonesia.

Casey-Maslen, S. (Ed.). (2014). *Weapons under international human rights law*. Cambridge University Press.

Christianto, H. (2010). Batasan dan Perkembangan Penafsiran Ekstensif dalam Hukum Pidana. *Pamator Journal*, *3*(2), 101-113.

Dinstein, Y. (2012). The principle of distinction and cyber war in International Armed Conflicts. *Journal of Conflict and Security Law*, *17*(2), 261-277.

Dörmann, K. (2004, November). Applicability of the Additional Protocols to computer network attacks. In *International Expert Conference on Computer Network Attacks and the Applicability of IHL, Stockholm* (p. 3).

Droege, C. (2011). No legal vacuum in cyber space. *ICRC, Interview*, *16*.

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. *O cial Journal of the European Union*.

Gervais, M. (2012). Cyber attacks and the laws of war. *Berkeley J. Int'l L.*, *30*, 525.

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.

House of Commons Defence Select Committee. (2012). Defence and Cyber-Security. *Sixth Report of Session*, *13*, 11.

Joyner, C. C., & Lotrionte, C. (2001). Information Warfare as International Coercion: Elements of a Legal Framework. *European Journal of International Law*, *12*(5), 825-865.

Kellenberger, J., & Spoerri, P. (2012). International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011.

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

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996

Lewis, J. A. (2013). *Conflict and negotiation in cyberspace*. Washington, DC: Center for Strategic and International Studies.

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

Martin, F. F., Schnably, S. J., Wilson, R., Simon, J., & Tushnet, M. (2006). *International human rights and humanitarian law: treaties, cases, and analysis*. Cambridge University Press.

Melander, G. (2006). *Essays in Honour of Göran Melander* (Vol. 26). Martinus Nijhoff Publishers.

Melzer, N. (2011). *Cyberwarfare and international law*. United Nations Institute for Disarmament Research.

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

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

Rogers, A. P. V. (2013). *Law on the Battlefield*. Oxford University Press.

Saleem, M., & Hassan, J. (2009). " Cyber warfare", the truth in a real case. *Project Report for Information Security Course, Linköping Universitetet, Sweden*.

Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International Review of the Red Cross*, *84*(846), 365-399.

Schmitt, M. (2012). Classification of cyber conflict. Journal of conflict and security law, 17(2), 245-260.

Smits, T. V. (2000). *Computer Network Attack As a Tool for the Operational Commander*. NAVAL WAR COLL NEWPORT RI JOINT MILITARY OPERATIONS DEPT.

Swanson, L. (2010). The era of cyber warfare: Applying international humanitarian law to the 2008 Russian-Georgian cyber conflict. *Loy. LA Int'l & Comp. L. Rev.*, *32*, 303.

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

Jensen, E. T. (2002). Unexpected consequences from knock-on effects: a different standard for computer network operations. *Am. U. Int'l L. Rev.*, *18*, 1145.

Wamala, F. (2011). ITU National Cyber Security Strategy Guide. *International Telecommunications Union*, *11*.

Zainal A. Hasibuan, Indonesia National Cyber Security Strategy: Security and Sovereignty in Indonesia Cyberspace. Dewan Teknologi Informasi dan komunikasi Nasional. 2013

http://www.cisco.com/c/dam/en/us/products/collateral/security/security-benchmark-study-government.pdf.
https://ccdcoe.org/cyber-definitions.html
http://www.theguardian.com/technology/2007/nov/29/hacking.news
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
http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang
http://www.pelitaonline.com/read/iptek/internasional/28/17447/virus-flame-serang-ribuan-komputer-di-iran/,
http://www.economist.com/node/16478792
http://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm
http://rt.com/news/mini-flame-malware-kaspersky-519/
http://inet.detik.com/read/2012/01/20/105656/1820779/323/7-negara-asean-yang-paling-sering-kena-serangan-web/).
http://www.merdeka.com/teknologi/hacker-china-incar-militer-negara-negara-asia-indonesia-termasuk.html
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/
http://teknologi.news.viva.co.id/news/read/166993-trojan-scada-hantui-iran-indonesia-india
http://www.thefiscaltimes.com/Articles/2013/03/11/The-Coming-Cyber-Attack-that-Could-Ruin-Your-Life
http://www.antaranews.com/berita/399394/cyber-army-antisipasi-cyber-warfare
https://www.icc-cpi.int/resourcelibrary/official-journal/elements-of-crimes.aspx#article8-2a-iv
http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2015_Ch9.pdf
https://ihldatabases.icrc.org/applic/ihl/ihl.nsf/b466ed681ddfcfd241256739003e6368/d80d14d84bf36b92c12563cd00434fbd

List of Authors:

Anang Setiyawan
Universitas Sebelas Maret, Jl. Ir,
Sutami No. 36A, Surakarta,
Jawa Tengah, Indonesia
Email: anang.setiyawan.sh@gmail.com

Jamal Wiwoho
Universitas Sebelas Maret, Jl. Ir,
Sutami No. 36A, Surakarta,
Jawa Tengah, Indonesia

Rahayu
Universitas Sebelas Maret, Jl. Ir,
Sutami No. 36A, Surakarta,
Jawa Tengah, Indonesia
Email: