Tallinn manual: Cyber warfare in Indonesian regulation

B Pratama and M Bamatraf

1,2 Business Law Department, Bina Nusantara University, Kijang Campus. Jln. Kemanggisan Ilir III No. 45, 11480 Jakarta Barat - Indonesia

Email: bptama@binus.ac.id

Abstract. Advances in communication information technology have made various infrastructures dependent on cybernetics technology. However, there are threats to the system. One of the threats discussed in the context of the study of international humanitarian law is cybernetics war, which is carried out by high entities such as the state. The threat is coordinated with the armed forces or military in order to gain an advantage over the opponent. Recognizing that there are ever-evolving and very dynamic threats to the sovereignty of the state and nation, in this case by considering advances in internet technology, the government has formulated regulations regarding cyber defence as an effort to overcome cyberattacks that cause disruption to the implementation of national defence, so that it can realized cyber defence (cyber defence). In general, there have been a number of national laws and regulations governing matters relating to activities in cyberspace. The research method of the paper used normative legal research to collect and analyse legal material regarding two main concepts, namely: cyber warfare regulations and information regulations. The nature of legal research was to provide prescription on legal concept or legal phenomenon. The paper finds out that Tallinn Manual is a legal concept that give an instruction to respond cyber-attack, in which the concept can be adopted. In the meantime, in legal vacuum of cyber warfare regulation, the concept inside Tallinn Manual can be interpret to the existing law in Indonesia. Findings in the paper indicates that cyber-attack according to existing regulation can be classified into three categories, namely: ordinary attack, middle attack or terrorism, and massif attack or cyber warfare.

Keywords: Tallinn manual, cyber warfare, Indonesian regulation

1. Introduction

The cyber warfare incidents in Estonia and Iran are concrete examples for academics and experts working in that field to be able to make national and international policies [1]. In recent years, countries and international organizations see urgency and are aware of threats and challenges that need to be addressed. The Tallinn Manual was established on the International Law Applicable to Cyber Warfare which was the result of the endeavours of an independent international expert group and was invited by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE). The Tallinn Manual was formed for three years to examine how international legal norms still apply to new forms of warfare. The Tallinn Manual pays special attention to aspects of jus ad bellum, namely international law governing the use of violence and also jus in bello. The Tallinn Manual is not an official document and has no binding capacity, but it is of a scientific opinion and serves as a state reference for arrangements related to cyber operations [2].
Tallinn Manual 1.0 emphasis cyber-to-cyber operations such as cyber operations on a country’s critical infrastructure or cyberattack that target system control from enemies. The Tallinn Manual is not intended for legal issues related to kinetic-to-cyber operations, such as an air strike that bombs a cyber control centre, which has been regulated in the provisions of armed conflict. Tallinn Manual 1.0 is neither intended for cyber securities as is generally understood. Cyber espionage, theft of intellectual property rights, and criminal activity in cyber space, although are serious issues for the state, are not included in the scope of regulation in Tallinn Manual 1.0. Utilising treaties, law cases, and other sources, Tallinn Manual 1.0 produces 95 (ninety-five) black-letters rules that can be used as guidelines for countries in cyber warfare conditions, including the provisions of cyber operations in neutral territory [3].

According to the Tallinn Manual which has now been ratified and took effect on March 2013 by NATO cyber defence in Estonia, American cyber-attacks on Iran is categorised as a form of "Use of Force". According to The Tallinn Manual on the International Law Applicable to Cyber warfare Rule 11: "Use of Force’ is defined as “Acts that kill or injure persons or destroy objects or damage objects are unambiguously uses of force”. According to the United Nation Charter, the use of force (violence) is prohibited, except in self-defence. "With the use of force by the United States, it can be said that it is an American hostility act against Iran which can be said to be the first sign of conflict as stated in international humanitarian law in the 1949 Geneva Conventions.

The development of cyber law reached a certain level of maturity by starting to think about the enactment of public international law into the area of cyber operations. Last January 2017 the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations with General Editor Michael N. Schmitt was published by Cambridge University Press. If Tallinn Manual 1.0 emphasizes the discussions on cyber operations related to cyber warfare, Tallinn Manual 2.0 highlights cyber activities during peacetime by emphasizing cyber events facing the country in day-to-day operations that are below the level of cyber operations. By using treaties, case law and other sources, Tallinn Manual 2.0 publishes 154 (one hundred fifty-four) black-letters rules [4].

In 2019 Indonesian government is discussing cyber security to be articulated as legislation. Also, within Indonesian regulation Tallinn Manual is not regulate specifically. In the absence the rule of law in terms of cyberattack or cyber war, the referral concept can be interpreted to the existing law that have closely related to the cyber space law. Although, to become governing law, Tallin Manual regulation must be fulfilled some of requirement, namely: sign by the country member, ratification, obeyed and execute by the country member.

In regards of Tallinn Manual, Schmitt argue that Cyberwar do not take place but existing law and can be established through legal interpretation [5]. Correspond to the legal context, doctrinal method or normative legal research can be used as a tools to interpret the Tallin Manual through the concept of cyberwar as sub-field in international law [6]. In doctrinal research the analysis is to understand and to draw legal concept coherently among various regulation [7]. Depart from the nature of the research, basic understanding of the concept will be point to a definition then will be relate to the concept in academic paper to have comprehensive understanding to prescribe cyber warfare from the perspective Indonesian regulation.

2. Conceptual framework
2.1. Cybercrime
Cybercrime is not specifically defined in the Convention on Cybercrime. However, if it is seen from the sub-section of the convention, we can conclude that cybercrime has several types of criminal offenses, namely offenses against the confidentiality, integrity and availability of computer data and systems, computer-related offenses, content-related offences, and offenses related to infringements of copyright and its related rights that can be harm the society. The term of computer crime is still not uniform, some scholars mention the terms "computer abuse", "computer fraud", "computer-related crime", "computer assisted crime" or "computer crime", but in the end the term that is widely used is "computer crime due to its commonly used in international relations [8]. Main concept to describe act of crime in cyberspace
terminology as if computer crime, or crime that uses a computer (computer-related crime) in legal perspective will affect to the legal consequences. In so, our opinion for cybercrime is the crime that happen in cyberspace, and computer-related crime is for conventional crime that use computer as a tool of crime.

In terms of terminology cyber, on Information and Electronic Transaction law section explanation, there is cyber terminology, but written: law of information technology, virtual world law, and law of mayantara [9]. The condition described that Indonesian law is not explicitly accommodate cyber as a concept of law, but rather choose terminology information. Otherwise, in many textbook of cyber law, common terminology is cyber, and cyber is a space that needs law inside the space to regulate the people inside the space [10].

In some countries, the use of the term still varies, for example, The British Law Commission uses the term computer fraud as computer manipulation in any way carried out in bad faith to obtain money, goods or other benefits or is intended to cause harm to others. Whereas U.S computer crime manual uses the term "computer crime", the Franken Commission in the Netherlands uses the term "cybercriminaliteit" or a crime on the Internet [11]. In short, each country has their reasons for using these terms, but with the development of the internet and telecommunications networks, the term widely used is "cybercrime".

Cybercrime is carried out through computers in cyberspace or computer networks that have high-speed access so that this crime becomes a high-level crime that changes the concept of conventional crime. Apart from access and high speed, cyberspace that is not physically seen makes interactions between individuals or groups as cybercrime actors freer in carrying out their actions, and thoughts that are considered illegal in the real world can be spread through cyberspace. This gives way to the birth of cyber terrorism due the freedom it bestows upon someone to publish his illegal ideas on cyberspace [12].

From the characteristics, it is clear that the perpetrators of crime today choose to carry out their actions through this medium of cyberspace. In addition to their freedom and ease in carrying out criminal acts, the law applicable to cyberspace also does not explicitly have universally recognized limits, USDOJ (United States Department of Justice), for example, considers that penalties that apply in real space should also apply in cyberspace, because USDOJ considers computers to be just media for crimes that still have implications in the real world [13]. In contrast, some experts adhere to the opposite principle in essence it states that the law in force in real space is irrelevant if it is imposed on cyber space.

2.2. Cyber attack
Cyber-attack by definition is a cyber operation that is either offensive or defensive in nature, intended to change, delete, destroy or deny access to computer data or software. This action is carried out with aims of, among others: 1) Making propaganda or fraud, 2) Disrupting the function of computers, targeted computer system networks and certain infrastructure operator computers. 3) Give the impact of physical damage to computers, computer systems or networks [14].

Within military context, cyber-attacks can be perceived as a separate operation or used in operations that combine conventional (kinetic) attack operations. A cyber-attack is used for harmless effects (such as site destruction), which causes fatal damage or impacts by producing misinformation in military operations or to cause major disruption to services and physical and material damage to property as well as loss of life. Cyber-attacks are conveyed through cyberspace but cannot always be carried out through a network and can make information systems or infrastructure control systems a target [15]. For an example on infrastructure control, SCADA system which operates the infrastructure. If the system is damaged, the consequence is that physical interference or damage can occur. Therefore, for security reasons, the attack on SCADA system was launched from a closed network or installing malware from agents who have close access to the system.

The methods used to carry out cyber-attacks vary; damage the hardware (chipping) or flood the system with so much information that it causes it not to function. Software formed to disrupt the function
of a computer that includes Trojan horses, logic bombs, viruses and computer worms [16]. To be able to install the software, it is launched on a computer by chipping, hacking, using a portable storage device or accidentally downloading from a site or email attachment [17].

2.3. Cyber warfare

Cyber-Warfare in Indonesian means Cybernetics War. Etymologically the term is divided into two namely cybernetics/cyber and war/warfare. UNTERM (United Nations Multilingual Terminology Database) has the definition of the full understanding of cyber-warfare as "The offensive and defensive use of information and information systems to deny, exploit, corrupt or destroy an adversary's information, information-based processes, information systems and computer based networks while protecting one's own. Such actions are designed to achieve advantages over military or business adversaries [18].

The UN organ in addition to UNTERM which also provides understanding of cyber-warfare is UNICJRI (United Nations Interregional Crime and Justice Research Institute). UNICJRI defines cyber-warfare as any action by a nation-state to penetrate another nation's computer networks for the purpose of causing some sort of damage. UNICJRI explains that cyber-warfare is carried out by countries to destroy / damage one computer network system other.

It is very important beforehand to know that the notion of cyber-warfare cannot be equated with cybercrime, cyber-espionage, and cyber-vandalism even though all of them have in common the use of cyber technology. Cyber-Crime is an act of crime (criminal) to benefit from the existence of cyber technology by violating the national law of a country, it can be said that cybercrime is more in the realm of criminal law or international criminal law.

2.4. Tallinn manual

The Tallinn Manual (originally titled, The Tallinn Manual on the International Law Applicable to Cyber Warfare) is an academic study, not binding on how international law (specifically jus ad bellum and international humanitarian law) applies to cyber conflicts and cyber warfare. Between 2009 and 2012, the Tallinn Manual was written at the invitation of the Tallinn Cyber Defence Cooperative of Excellence Centre based in Tallinn by an international group of about twenty experts. In April 2013, this manual was published by Cambridge University Press.

In the Tallinn Manual of the International Applicable to Cyber Warfare in Rule I. Sovereignty states that a state may exercise control over cyber infrastructure and activities within its territory [19]. The provision explains that a country can exercise control over cyber cyberspace infrastructure and cyber/cyberspace activities that are within its sovereign territory.

From the definition given by Bodley and the provisions in the Tallinn Manual it can be said that when a State has capabilities in terms of cyber/cyberspace infrastructure, the state has sovereignty in cyber/cyberspace and general conditions contained in international law regarding cyber/cyberspace for can be said as a fulfilled domain.

If there are interests that are protected or targeted such as cyber-based infrastructure, some countries already have or will have the capability of defence or attack against cyber whether or not they are in a military organizational structure. Attack in the virtual world (cyber/cyberspace) coordinated by the state in order to gain political and military superiority over their enemies. Hence, cyber/cyberspace becomes the domain/dimension of war/armed conflict only after land, sea, air land in the future.

Cyber-Warfare actors can provide answers whether an attack (cyber-attack) can be categorized as cyber-warfare or not. And more broadly can identify cyber-warfare whether including international armed conflicts or non-international armed conflicts. The International Group of Experts in the Tallinn Manual agree that a conflict is an international conflict if two or more countries are involved as conflicting parties or when non-state actors are under the overall control of the state of one country involved in hostilities one another.

In practice, it is very difficult to ascertain whether a country controls the cyber activities of these non-state actors (hackers or crackers). Non-state actors means: those who are allowed to be given orders
by the state such as the military, hacker groups/hackers that are sponsored by the state to attack (cyber-attack) against computer systems in other countries.

In Tallinn Manual Rule 43, the concept based on Article 51 (4) Additional Protocol I of the Geneva Conventions of 1949 states that it is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be: (a) directed at a specific military objective; (b) limited in their effects as required by the law of armed conflict.

Based on the provisions of Rule 43 Tallinn Manual, cyber-attack by NATO is an indiscriminate attack because it intentionally sends malware that can be expected to be dangerous to civilians and civilian objects (Article 51 (5) (b)). Besides, weapons in the form of malware in the cyber-attack cannot limit its attacks (uncontrollable effects) to military targets only.

Furthermore, experts in the Tallinn Manual argue that the deaths of civilians, the wounding of civilians, the destruction of civilian objects, or the combination of these are collateral damage. They also categorise collateral damage into direct effect and the indirect effect. Direct effects are the immediate, first order consequences, unaltered by intervening events or mechanisms. By contrast, indirect effects are the delayed and/or displaced second, third, and higher order consequences of action, created through intermediate events or mechanisms.

Understanding the direct effect is the effect that is directly felt when an attack occurs, then the indirect effect is the effect that is delayed, or it is the implication of the attack because it is near the object of attack. Collateral damage is a factor in a proportional calculation including the indirect effects that must be estimated by the parties before carrying out an attack by looking at planning, approval and implementation. In the context of cyber-warfare attacks that cause collateral damage such as attacks (cyber-attack) on Global Positioning Satellite (GPS), the attacker can assume the satellite is attacked because it is an object/military target that provides effective benefits to the enemy military. On the other hands, GPS satellites are also used by civilians for transportation services such as civilian commercial airplane navigation. Hence, attacker before carrying out cyber-attacks on the GPS satellite needs to consider proportionally so as not to cause collateral damage as referred to above.

3. Cyber warfare regulation in Indonesia

Recognizing that there are ever-evolving and very dynamic threats to the sovereignty of the state and nation, in this case by considering advances in internet technology, the government has formulated regulations regarding cyber defence as an effort to overcome cyber-attacks that cause disruption to the implementation of national defence, hence, launches a cyber defence (cyber defence). In general, there have been a number of national laws and regulations governing matters relating to activities in cyberspace, namely: telecommunication law, defence and security law, national defence law, armed force law, national police law, information and electronic transaction law, and antiterrorism law. In relation to Tallin Manual Coverage per se the coverage of cyber operation in not explicitly describe on what is cyber operation in Indonesian regulation, therefore Tallinn Manual 2.0 can become a guidance to follow [20].

From the regulation above, there is main difference from ordinary cybercrime then cyber-attack or cyber war. The difference is lies on the impact and the object of the cyber-attack. Cyber operation according to International law can be categorized: (a) intensity of the cyber-attack, (b) use of force, (c) action to maintain or restore international peace and stability, (d) and armed attack [9]. There for the act of cyber-attack is the same with ordinary or personal attack, but the impact of the attack that can be different.

Cyber-attack according to Indonesian law is seen as a crime and is in the domain of national security (the authority of law enforcement/police). In the Criminal Code for example, it does not specifically regulate matters relating to cyberspace. Although, the antiterrorism law create guidance that attack to vital object: place or building that have value on economy, politic social, culture and defence and security can be classified as terrorism action [22], and for the electronic or cyber can be junto to Information and Electronic Transaction Law No. 19/2016 as amendments to the Law No. 11/2008.
The crimes regulated in ITE law are very diverse, ranging from crimes related to internet technology activities such as misuse of access, interception, illegally entering computer systems or electronic systems, to committing criminal acts in the form of destruction, change, removal and manipulation of electronic data information [21]. In a more specific regulation, a cyber-attack is formulated in the Minister of Defence’s Regulation No. 82 of 2014 as "all forms of actions, words, thoughts, whether intentionally or unintentionally carried out by any party with any motive and purpose, which are carried out at any location, which are targeted at the electronic system or its contents (information) or equipment that relies heavily on technology and natural networks of any scale, to vital and non-vital objects in the military and non-military sphere, which threaten the country's sovereignty, territorial integrity and national safety”.

This cyber-attack can occur when the intensity and scale of cyber threats increase and change from the level of potential threats to become factual. This generally takes the form of actions aimed at entering, controlling, modifying, stealing or destroying or destroying or paralyzing information systems or assets. This action can take the form of cyber warfare (cyber warfare) carried out deliberately and coordinated with the aim of disturbing the sovereignty of the state; or in the form of cyber-disruption, which is carried out unintentionally, is passive and small-scale.

According to the Minister of Defence Regulation No. 82/2014 in article 2.2.a. was stated: threats to state sovereignty caused by cyber threats can originate from internal and external sources; intelligence activities; extremist organizations; "hack activists" group; organized crime groups; or originating from competition, hostility and conflict. Further, it also lists cyber threats that may occur, such as threats to the hardware (hardware threat) caused by the installation of certain equipment that functions to carry out certain activities in the system, so that the equipment is a disruption to the network system and other hardware, like jamming and network intrusion.

Another cyber threat is the threat to software (software threat). This threat is usually done by sending particular software via electronic mail that functions to carry out activities such as information theft, information destruction, information manipulation, and other activities. Cyber threats can also be in the form of data or information threats that result from the dissemination of certain data or information aimed at carrying out certain interests such as those carried out in information warfare, including propaganda activities. By looking at the contents of the said Minister of Defence Regulation, there is no limit to determine whether a cyber-attack, including cyber terrorism can be qualified as an act of war or armed attack. This is deemed necessary to formulate a working definition and scope of the cyber war. Failed to do so, it can be ill-used as a basis for political leaders to enable military leaders or warlords to take appropriate action in connection with existing cyber-attacks [22].

In addition to the Minister of Defence Regulation, the Minister of Defence Decree No.KEP/1008/M/V/2017 concerning 2018 National Defence Policy, the national defence policy is realized by establishing national infrastructure and a universal defence system to face the threat of cyberattacks both military and non-military by integrating defence information systems country; optimize cyber defence in accordance with cyber defence guidelines; encourage relevant ministries or institutions in the mastery of defence technology and human resource development and infrastructure development in the field of technology and communication for national defence.

4. Conclusion

Cyber-attack regulation in Indonesia still partially regulate, some of regulation regarding military issue in on ministry of defence, and for the public crime is regulate under ITE law and antiterrorism law. Main question for describing state cyber-attack that has been written in Tallinn manual, can be determine by the effect of the cyber-attack. By this condition, if the impact of cyber-attack is massif and the target is on vital object like strategic infrastructure, then the action can be merit as cyber-attack that threatening national defence.

Based on existing law, cyber-attack in Indonesia can be divided into three categories condition, namely: (1) ordinary attack, that aim to an individual, (3) vital object attack but not doing cyber operation, that can be classified as terrorism action, and (4) warfare attack, that massif and runs by state.
Within Indonesian rule condition that cyber-attack was regulated partial, it is cannot be said that Indonesian law have no regulation regarding cyber-attack. By the condition of law, can be interpret that Indonesia regulation is measuring the condition and the impact of cyber-attack. For cyber-attack that have massive impact, is an act that can be defined as threatening national defence, then the applicable law needs to consider the aspects of humanitarian law, including the determination or classification of "armed conflict" and who are the actors who can be considered to participate directly in hostilities. It is therefore recommended that policies on cyber defence need to include aspects of the humanitarian law in the future for regulating cyber war and/or cyber security.

References

[1] Dinnis H H 2012 CYBER WARFARE AND THE LAWASOF WAR. London: Cambridge University Press.
[2] "EJIL:Talk! Blog of the European Journal of International Law," 15 April 2013. [Online]. Available: https://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/. [Accessed 14 June 2020].
[3] Yuniarti S. "Business Law Bina Nusantara University," October 2017. [Online]. Available: https://business-law.binus.ac.id/2017/10/30/cyber-warfare-tallin-manual-1-0/. [Accessed 13 June 2020].
[4] Yuniarti S. "Business Law, Bina Nusantara University," November 2017. [Online]. Available: https://business-law.binus.ac.id/2017/11/30/cyber-operation-tallin-manual-2-0/. [Accessed 14 June 2020].
[5] Schmitt M N. 1999. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Columbia Journal of Transnational Law, 37 911.
[6] Razak A A. 2009. Understanding Legal Research, Integration and Dissemination, p. 20.
[7] McCrudden C. 2006. Legal Research and the Social Science, Oxford Legal Studies Research Paper, No. 33, p. 633.
[8] Rugge F. 16 July 2018. "Italian Institute for International Political Studies," [Online]. Available: https://www.ispionline.it/en/pubblicazione/cybercrime-and-international-relations-20996. [Accessed 15 June 2020].
[9] "Law No. 11 regarding Information and Electronic Transaction, 2008."
[10] Lessig L 2006 CODE VERSION 2.0. New York: Perseus Books, 2006.
[11] Nationaal Cyber Security Centrum, Ministerie van Veiligheid en Justitie, January 2012. [Online]. Available: https://europadecentraal.nl/wp-content/uploads/2013/02/Handreiking-Cybercrime.pdf. [Accessed 15 June 2020].
[12] Athira U S M T.2015. "Authorsip Analysis: Technoques and Challenges." in New Threats and Countermeasures in Digital Crime and Cyber Terrorism, Hershey, Information Science Reference, p. 188.
[13] Katyal N K 2001. "Criminal Law in Cyberspace," University of Pennsylvania Law Review, 149, p. 1085.
[14] Goldsmith J. 2013. How Cyber Changes the Laws of War, The European Journal of International Law 24 133.
[15] Heaton J R 2004 REEXAMINING THE STATUS OF CIVILIANS ACCOMPANYIN THE ARMED FORCES. Washington DC: George Washington University.
[16] Morth T A. 1998. Considering Our Position: Viewing Information Warfare as a Use of Force Prohibited by Article 2(4) of the U.N. Charter. Case Western Reserve Journal of International Law 30 591.
[17] Melzer N 2011 "United Nations Institute for Disarment Research," [Online]. Available: https://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf. [Accessed 15 June 2020].
[18] Andress S Wd J. 2013. THE BASIC OF CYBER WARFARE; UNDERSTANDING THE FUNDAMENTALS OF CYBER IN THEORY AND PRACTICE. Waltham: Elsevier and Book Aid International.
[19] Schmitt M N. 2013. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE. London: Cambridge University Press.

[20] Jensen E T. 2017. The Tallinn Manual 2.0: Highlight and Insight. Georgetown Journal of International Law, 48, 755.

[21] Kosmas Pipyros C T L M D G T A. 2018. A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, Computer & Security 74, 374.

[22] Indonesian Government Regulation No. 1 regarding Antiterrorism, 2002.

[23] Anang Setiyawan J W R. 2018 Strengthening Indonesia’s Policy on National Cyber Security to Deal with Cyberwarfare Threat, South East Asia Journal of Contemporary Business, Economic and Law 5, 15.

[24] Alan Cole P D R M D M. 2017. "Sanremo Handbook of Rules of Engagement." 11 [Online]. Available: http://iihl.org/wp-content/uploads/2017/11/ROE-HANDBOOK-ENGLISH.pdf. [Accessed 15 June 2020].