Padjadjaran Journal of International Law
ISSN: 2549-2152, EISSN: 2549-1296
Volume 5, Number 1, January 2021

The Beginning of the International Humanitarian Law Application to Cyber Attack: The Status of Rule 30 Tallinn Manual 1.0

Iradhati Zahra,* Diajeng Wulan Christianti**

ABSTRACT

Technological development has given rise to new means and methods of warfare such as cyber- attack and can potentially have devastating humanitarian consequences. In times of armed conflict, International Humanitarian Law (IHL) limits certain use of weapons, however, it is questionable whether an armed conflict exists in the situation where cyber-attack is employed alone. In 2007, Estonia suffered severe damages due to cyber-attacks that were equal to the damages caused by kinetic weapons. Yet, there is a debate on whether or not IHL applies in the Estonia case due to the shortage of a kinetic weapon. The Estonia case has generated NATO and other states to draft a cyber-warfare manual (Tallinn Manual 1.0) that, in its Rule 30, affirms the IHL applicability in the case of only cyber-attack. Due to the importance of this Rule, this article argues that Rule 30 shall be considered as a legally binding provision in the form of customary international law. This Rule has satisfied widely practiced and opinio juris elements although it is not in an ideal condition. According to Grotian Moment Theory, the formation of a new customary international law can be accelerated in times of a fundamental change as can be seen in the practice of customary air and space law.

Keywords: Customary International Law, Cyber-Attack, Grotian Moment Theory, IHL, Tallinn Manual 1.0

Awal Pemberlakuan Hukum Humaniter Internasional pada Serangan Siber: Status Rule 30 Tallinn Manual 1.0

ABSTRAK

Perkembangan teknologi telah melahirkan cara dan metode berperang yang baru seperti serangan siber dan dapat berpotensi menimbulkan kehancuran umat manusia. Hukum Humaniter Internasional (HHI) membatasi penggunaan senjata tertentu saat perang, sayangnya penerapan hukum ini masih dipertanyakan dalam kasus yang hanya melibatkan serangan siber. Tahun 2007 Estonia menderita kerugian akibat dari serangan siber yang tingkat keparahannya dapat disamakan dengan serangan kinetis. Namun, fakta bahwa serangan tersebut tidak melibatkan senjata kinetis melahirkan perdebatan perihal penerapan HHI. Kasus Estonia telah mendorong NATO dan negara-negara lainnya untuk merumuskan Manual tentang Perang Siber (Tallinn Manual 1.0) yang mengkonfirmasi penerapan HHI untuk kasus yang hanya melibatkan serangan siber. Pentingnya pengaturan dalam Pasal 30, artikel ini berpendapat bahwa pasal tersebut harus memiliki kekuatan hukum mengikat dalam bentuk aturan

* Policy Analyst Intern at Aimpact Global LLC, 1717 N STREET NW, SUITE 1, Washington, District of Columbia, 20036, iradhatizahra@gmail.com.

** Lecturer of the Faculty of Law Universitas Padjadjaran, Jl. Imam Bonjol No. 21 Bandung 40132 Indonesia, e-mail: wulan.christianti@unpad.ac.id.

hukum kebiasaan internasional. Pasal 30 telah memenuhi unsur hukum kebiasaan internasional yakni praktek negara yang luas serta *opinion juris*. *Grotian Moment Theory* menyatakan bahwa pembentukan norma hukum kebiasaan internasional baru dapat dipercepat karena adanya perubahan yang fundamental seperti yang dipraktekan dalam norma hukum kebiasaan ruang angkasa.

Kata Kunci: Hukum Kebiasaan Internasional, Hukum Humaniter Internasional, Serangan Siber, Tallinn Manual 1.0, Teori Grotian Moment

A. INTRODUCTION

The fast-paced technology brings a massive change to many aspects, including the application of cyber-weapon to attack cross-border states without actually entering or invading their territories. This can be seen in practice such as the 9/11 tragedy that was started from hacking through the Pentagon; cyber-attack in Estonia in 2007; a malware attack in Iran (Stuxnet case); and cyber-attack in Georgia v. Russia.[1] Those events, particularly the case of Estonia, have generated the need of the international community to have adequate rules about the limits of the use of cyber as a weapon both in times of peace and war.

It was the first time in history that a state, Estonia, suffered damage and destruction of infrastructure only due to the employment of cyber-attack alone.[2] The attack was launched by Nashi Youth Group (NYG), a youth democratic organization from Russia, that was allegedly supported by the Russian Government.[3] Estonia was incapable of responding to those attacks hence it requested support from North Atlantic Treaty Organization (NATO) and ENISA.[4] Although the damage is severe and Russia allegedly involved in that attack, it is not clear whether the use of only non-kinetic weapons such as cyber is sufficient to trigger the applicability of IHL. In practice, for as long as the kinetic weapon is employed, IHL directly applies in the case of hostility between states according to the Common Article 2 of Geneva Convention 1949 and Article 49 (1) Additional Protocol I 1977. However, those provisions are silent with regard to cyber-attack that involves the non-kinetic weapon alone.

Cooperative Cyber Defense Center of Excellence (CCD COE), an organization under NATO, facilitated experts, lawyers, scholars, and other stakeholders to draft a Manual on the International Law Applicable to Cyber Warfare called Tallinn Manual 1.0. This manual was finally concluded in 2013[5] and compiled and edited by Michael N. Schmitt, an expert in cyber. The Manual is accompanied by the opinions of the drafter as the commentaries.[6] Tallinn Manual 1.0 discusses international law related to cyber-warfare that includes jus ad bellum and jus in bello.[7] Rule 30 of Tallinn Manual 1.0 defines cyber-attack and provides further detail regarding the threshold of cyber-attack that could trigger the beginning application of International Humanitarian Law (IHL). This Rule firmly states that any cyber activity below the level of use of force could not be considered as a part of IHL as

---

1 Schmitt, Michael N. (ed). *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013.

2 Schimdt, Andreas. "The Estonian Cyber Attacks". *The Fierce Domain Conflicts in Cyberspace 1986-2012*, edited by Jason Healey. Atlantic Council, 2013, pp. 174 -193.

3 Herzog, Stephen. "Revisiting the Estonian cyber-attacks: Digital threats and multinational responses." *Journal of Strategic Security,* vol. 4, no.2, 2011, pp. 49-60.

4 *Ibid.,* at 54.

5 Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law,* vol. 48, 2017, pp. 735-778.

6 *Ibid.,* at 38.

7 Schmitt, *supra* note 1, at 18.

in this manual.[8] In other words, there is a threshold between cyber-operations in terms of IHL and cyber-operations in terms of cybersecurity. The latter only harms cyber-security such as cyber-spy, stealing of Intellectual Property, credit-scamming, etc.[9] Those examples reflect the threshold between cyber-operation that can trigger the IHL applicability as regulated in Tallinn Manual 1.0 and cyber-operations in terms of cyber-security provided in Tallinn Manual 2.0. Referring to Rule 30 of Tallinn Manual 1.0, it can be concluded that cyber-attacks in Estonia met the threshold and hence could trigger the IHL applicability. The case of Estonia is different from other cyber-attack such as the Stuxnet case in Iran and the case of Georgia v. Russia. This is because there were ongoing armed conflicts in both of the latter cases that employed also other conventional weapons.[10]

This article starts with the elaboration of the elements of Rule 30 Tallinn Manual 1.0 to seek whether it provides more specific rules concerning the threshold of IHL applicability. After determining that this Rule provides a sufficient basis for the threshold of IHL applicability in the case of cyber-attack, it further examines the possibility of this rule to be considered as a legally binding norm. In this regard, this article tries to determine whether or not Rule 30 satisfies the element of customary international law. This article also supports its argument with the Grotian Moment Theory that has previously been used as a basis of other norms of international law that have similar nature with Rule 30 to satisfy the element of customary nature. It leads to the conclusion that even if Rule 30 may insufficiently meet both of the elements of customary international law, its specific nature together with the fundamental changes surrounding the circumstances that shape its rule into an important rule of international law are sufficient to accelerate this rule from soft law nature to customary nature of international law.

B. RULE 30 TALLINN MANUAL 1.0 AND THE THRESHOLD OF CYBER ATTACK: DOES IHL APPLY?

Rule 30 of Tallinn Manual 1.0 defines a cyber-attack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[11] There are at least three elements that need to be fulfilled to determine that a cyber- attack can trigger the beginning application of IHL, namely (1) a cyber-operation; (2) offense or defense; and (3) the expected impact on a person or object. Therefore, it is necessary to have a close examination of each of those elements.

1. The Element of Cyber-Operation

The element of 'cyber-operation' can be interpreted by using the grammatical method of interpretation. According to the Oxford English Dictionary (OED), 'cyber' is anything that is "connected with electronic communication networks, especially the internet".[12] The word 'operation' means "an act performed by a machine, especially a computer",[13] meanwhile in the military topic, "operation is a military activity".[14]

---

8 *Ibid.*

9 *Ibid.*

10 Tikk, Eneken, (*et.al.). International cyber incidents: Legal considerations*. Estonia: Cooperative Cyber Defence Centre of Excellence, 2010; Kagan, Kimberly. "Iran's Proxy War Against the U.S and the Iraqi Government". *Institute for the Study of War and weeklystandard.com,* Mei 2006 – 20 August 2007.http://www.understandingwar.org/report/irans-proxy-war-against-united-states-and-iraq. Accessed on 12th of November 2020.

11 Schmitt, *supra* note 1, at 91.

12 Oxford English Dictionary (OED), https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber. Accessed on 2nd of June 2020.

13 Oxford English Dictionary (OED), https://www.oxfordlearnersdictionaries.com/definition/english/operation?q=operation, Accessed on 2nd of June 2020.

14 *Ibid.*

Using a systematic or contextual method of interpretation, 'operation' can also include an operation in military activity by using a computer as their medium. It can be concluded that a 'cyber- operation' is an act involving computers and the internet as their medium, and this can apply to military activity as well. Those interpretation methods are supported by paragraph 1 of the commentary of Rule 30 of Tallinn Manual 1.0 states that this article could apply equally to both IAC and NIAC.[15]

2. The Element of Offense or Defense

This element is adopted from Article 49 (1) Additional Protocol I 1977. An act of violence using a cyber-attack should be applied equally in terms of offense or defense. However, the commentary of Rule 30 states that an attack should not only be limited to a kinetic attack but also has to be applied equally to a non-kinetic attack.[16] Such explanation does not exist in Article 49 (1) Additional Protocol 1 1977. Besides, paragraph 7 of this commentary article ascertains that attacking in offense or defense must be launched based on 'against the adversary'.[17] This is in line with Julia Grignon's opinion that an attack must be launched based on enmity.[18] It can be seen in the case of Estonia where the hostilities between Nashi Youth Group and the Estonian Government were reflected by their xenophobic atmosphere.[19] Therefore, the element of 'enmity' is met in this case and could legitimize the cyber-attack.

3. The Expected Impact on a Person or Object

This third element demonstrates that the Rule of 30 Tallinn Manual 1.0 provides a more detailed definition of attack compared to Common Article 2 Geneva Convention 1949 and Additional Protocol I 1977. This Rule specifies that the impact shall be physical both against the protected person or objects. It also affirms in paragraph 5 of commentary of Rule 30 stated that the effects should be an expected physical impact.[20] The word 'expected' means a cyber-attack is about to cause harm to a person or an object physically, even though the impact was not directly shown or felt by the target.[21] This rule adopted a 'general feeling' concept from Article 49 (1) Additional Protocol I 1977 in paragraph 1881 of its commentary. The 'general feeling' concept uses an analogy of mines that buried down into the ground is guaranteed to give a physical impact both for a person or an object. Although such impact has not been revealed, the attack is still considered to have been launched.[22] The mines analogy, paragraph 3 of commentary of Rule 30 Tallinn Manual 1.0, elaborated this with non-kinetic weapons in the same way with the mine analogy. According to that paragraph, a biological weapon; radiological weapon; and chemical weapon might not have a kinetical character to legitimate the attack, yet those three could cause harm to a person, both injured or dead, and still regulated as an attack under the existing IHL.[23] As well as those three weapons, the cyber-

15 Schmitt, *supra* note 1*,* at 91, para. 1.
16 *Ibid.,* para. 3.
17 *Ibid.,* para. 3.
18 Grignon, Julia. "The beginning of application of international humanitarian law: A discussion of a few challenges." *International Review of the Red Cross*, vol. 96, no. 893, 2014, pp. 139-162, at 139.
19 Yapici, Merve İrem. "What Role Did Nashi Play in Russian Internal Politics and Foreign Policy: A Formulator or an Implementer." *Review of International Law and Politics,* vol. 12, no. 2, 2016, pp. 101-137, at 101.
20 Schmitt, *supra note* 1, at 93, para. 5.
21 *Ibid.*
22 *Ibid.,* at 94
23 *Ibid.*

attack should be legitimized as an attack if they could give an expected physical impact both to person and object. Moreover, the 'general feeling' concept by a cyber-attack can be shown from the Case of Stuxnet in Iran since the cyber-attack was launched a year ago before Iran realized the attack.[24] Indeed, the cyber-attack gave massive physical damage to Natanz Nuclear Plant slowly that Iran didn't know for a year.[25]

Moreover, the commentary of Rule 30 Tallinn Manual 1.0 affirms cyber as a weapon by referring to the definition of a weapon in the AMW Manual. A weapon is "a means of warfare used in combat operations, including a gun, missile, bomb or other munitions, that is capable of causing either (i) injury too, or death of persons; or (ii) damage to, or destruction of, objects".[26] It can be concluded that the definition focuses on the physical impacts as a purpose of the attack. Therefore, Rule 30 of Tallinn Manual 1.0 confirms the legality of cyber as a weapon to attack either offense or defense.

Referring back to Estonia's case, the cyber-attack as means of hostilities between Russia and Estonia had caused severe physical such as the destruction of Tallinn's water supply and transportation railway and hence could be considered as attack under the Rule 30 of Tallinn Manual 1.0 and triggered the IHL applicability. In other words, Rule 30 of Tallinn Manual 1.0 had answered the problem of the threshold of a non- kinetic attack such as cyber that may trigger the beginning application of International Humanitarian Law.

Nevertheless, this emerging norm from Rule 30 of Tallinn Manual 1.0 could not be deemed as a legal basis for the cyber-attack in Estonia. Tallinn Manual 1.0 concluded in 2013, six years after the cyber-attack in Estonia. This case however is evidence that Rule 30 Tallinn Manual is important to fill the gap in the case of the threshold of non-kinetic attack for the IHL to be applied. It is necessary to see the possibility under international law for this Rule to be considered as a legally binding rule such as customary international law.

C. THE CUSTOMARY NATURE OF RULE 30 TALLINN MANUAL 1.0

Customary international law is one of the primary sources of international law besides a treaty and the eldest source of international law, yet the establishment of customary international law is quite tricky and debatable in the international community.[27] A customary international started from state practice that firstly did not codify or written, until its growth and adoption, then became more established to be customary international law.[28] However, the order of identification of a rule of customary international law existence could happen on the other way. An opinio juris could start firstly by a written text allegedly expressing a widespread legal conviction and then seeking to verify whether there is a general practice corresponding to it.[29]

Even though Tallinn Manual 1.0 consists of opinions from scholars and experts in cyber-warfare, the conclusion of the Tallinn

[24] Zetter, Kim. "An Unprecedented Look at Stuxnet, the World's First Digital Weapons". https://www.wired.com/2014/11/countdown-to-zero- day-stuxnet/. Accessed on 3rd of March 2020.

[25] *Ibid.*

[26] Boothby, William H. *Weapons and the law of armed conflict*. Oxford: Oxford University Press, 2016.

[27] Hoof, GJH Van. *Pemikiran Kembali Sumber-Sumber Hukum Internasional*. Bandung: Yayasan Obor Indonesia, 2000.

[28] Shaw, Malcolm N. *International law.* Cambridge: Cambridge University Press, 2017.

[29] Draft conclusions on identification of customary international law with commentaries, Adopted by the International Law Commission and submitted to the General Assembly (A/73/10), 2018.

Manual 1.0 derived from some incidents that occurred before the manual was drafted. This demonstrates the state practices element could have possibly been satisfied.

1. The Element of General Practices

The first element that commonly triggers the formation of customary international law is a general practice. General practice is how a state acts and behaves in their practice to form a custom, yet there has to be proof that a state actor could become general practice.[30] The proof could be legislation, judicial decisions, or a state act in the international community.[31] According to Malcolm N. Shaw, there is a dictum relevant to general practice as a part of the formation of customary international law, namely: length, generality, and constancy, and uniformity.[32] However, these factors could be proved its existence qualitatively by some judgments and advisory opinions decided by ICJ in accepting a custom without a certain length of time.[33]

First, according to Allain Pellet, there is no 'instant custom' if we see it from the length as a factor, yet ICJ implicitly objects to the length factor as one of the crucial factors.[34] Length does play a role in shaping general state practices to become a custom, yet it is not the most important element. Besides, it has already proven in some judgments and advisory opinions of ICJ that accepting a custom could be formed without a certain length of time.[35] Malcolm N. Shaw also supports that the length of general practice will depend on the condition of the cases and their nature.[36] His statement is proved from the emerging of customary international law in space law which can be considered progressive and fast-paced, this customary international law emerged from the fast-paced development of technology which only had by the United States and Uni Soviet (Russia).[37] This development demonstrates that the length element could be adjusted due to circumstances surrounding at that time and the nature of the emerging rules. It can be seen from the emergence of space customary law due to the rapid technology development.

Second, the generality factor in state practices has two criteria according to ICJ Judgment on North Sea Continental Shelf Case 1969 that are the involvement of states which have interest in that practices and the. generality or common understanding of those relevant states even if this practice is practicing in other regions.[38] Referring to the first criteria, the cyber-attack that occurred in Estonia involving the parties of hostilities that are Estonia and Russia. Other cases that employed the use of cyberweapons such as Georgia v Russia and the Stuxnet virus in Iran also involved both parties in the conflict.[39] Those three cases (that will be elaborated further in the following paragraphs) had fulfilled the first element of the generality factor. Furthermore, those three cases have caused severe physical impacts on civilian objects. This affirmed the threshold of cyber-attack as provided in the Rule 30 Tallinn Manual 1.0.

Third, the constancy and uniformity of such practices are the important

30 Shaw, *supra note* 29, at 82.
31 *Ibid.*
32 Pellet, Allain, "Article 38", *Commentary: The Statute of the International Court of Justice*, edited by Andreas Zimmermann et.al, Oxford University Press, 2012, pp. 676 -793.
33 *Ibid.*
34 *Ibid.*
35 *Ibid.*
36 Shaw, *supra* note 29*,* at 76.
37 *Ibid.*
38 Pellet, *supra note* 33, at 752.
39 Tikk, Eneken (et.al), *supra* note 11*;* Kagan, *supra note* 11.

factors of customary norm nature. In Nicaragua Judgement, the state practices in the international community have not been expected to have occurred perfectly.[40] It is possible to have little differences between states, yet these differences may be uniform by following some influencing states. De Visscher once said this using an analogy about the main road that has been built on a space. He said that if a majority of paths or streets are following one big tack or a road then it will become the main road.[41] His analogy is reflecting the emergence of customary international law from state practice, especially when it comes to influencing states involved and starting the 'main road'.[42] As an example, the emergence of customary international law in space has been built from state practice that had been practiced by the United States and Uni Soviet as influencing states, then followed by other countries. The competition between the United States and Uni Soviets had emerged general principles in space law, such as the common heritage of mankind; the right to passage and explore space without intervention; the prohibition to claim celestial objects.[43] Other states acknowledge it as mentioned in General Assembly Resolution XVII (1962) along with other general principles.[44] Those state practices reflect constancy and uniformity among other states and prove de Visscher's analogy about general practice.

The use of cyber-weapon in warfare had occurred in some cases besides the cyber-attack in Estonia in 2007. The Stuxnet Case in Iran also started from a virus called Stuxnet jointly created by the United States and Israel for the purpose to attack the Natanz Nuclear Plant in Iran.[45] Stuxnet was designed to destroy physically every piece of equipment controlled by the computer. It works by detecting a new well-functioned machine to be attacked until it stops.[46] The Stuxnet was launched in 2010 yet Iran has just realized the cyber- attack a year after the attack had launched.[47] This case has shown that the United States, as one of the highly influencing states, along with Israel has done a cyber-attack that could be considered as state practice. Even though the cyber-attack in the Stuxnet Case did not launch to trigger the beginning application of International Humanitarian Law since the United States and Iran had been involved in the proxy war long before the Stuxnet launched.[48]

The other case that employed cyber weapons was an armed conflict between Georgia v. Russia in 2008. The cyber- attack in this case launched by Russia to Georgia using DDoS.[49] The warfare between Russia and Georgia started in 1991 from the separatist movement in South Ossetia (one of Georgia's provinces), Russia had involved and supported the separatist movement until the cyber-attack in 2008 arose.[50] The cyber-attack was then

---

40 Pellet, *supra* note 33*,* at 753.

41 Shaw, *supra* note 29, at 79.

42 *Ibid.*

43 Ku, Julian, "Defining the Customary International Law of Outer Space", http://opiniojuris.org/2006/10/18/defining-the-customary-international-law-of-outer-space/. Accessed on 13th March 2020; Khatwani, Naman. "Common Heritage of Mankind for Outer Space." *Astropolitics,* vol. 17, no. 2, 2019, pp.89-103.

44 United Nations General Assembly Resolution on "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space ", 1962 (XVIII).

45 Zetter, *supra note* 25.

46 *Ibid.*

47 Parker, Diantha (*et.al.*). "Iran, the United States and the Political Seesaw", *The New York Times*,https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/07/world/middleeast/irantimeline.html #/#time5_211. Accessed on 27th of May 2020

48 Kagan, *supra note* 11.

49 Tikk, *supra* note 11, at 69.

50 *Ibid.,* at 67.

followed by military operation from both parties and a declaration of Mikheil Saakashvili, President of Georgia on August 9th, 2008.[51] Likewise the United States, Russia is one of the highly influencing states that possess high-technology and skilled human resources in technology. It shows that there are already two big states holding the cyber card in warfare. The constancy and uniformity reflected in the cases of Estonia, Georgia and Iran that have been attacked by the United States and Russia are in line with the shaping of space customary law.

Following those three cases, some states had taken real action in a matter of cyber-security or cyber armed forces, which help to validate the general practice of customary international law. China has formed a 'Blue Army Unit' under the Ministry of Defense, with a specific task to handle network and data, this unit has a different job with conventional armed forces.[52] North Korea also built a cyber-armed forces unit called 'Unit 121' under its Ministry of Defense.[53] Meanwhile, Russia gave authority to its federal agent called the Federal Security Service (FSB), to have a connection to all networks over their state.[54] Those states had proven their commitment to cyber-security matters by building cyber-armed forces or giving authority to their federal agent means that they realized the urgency to defend their countries by cyber. Their practices contribute to the formation, or expression, or rules of customary international law.

According to the ILC, a non-state actor such as an international organization could contribute to the formation, or expression, of rules of customary international law, but may be relevant when assessing the general practice.[55] International organizations are entities established and empowered by States (or by States and/or other international organizations) to carry out certain functions, and to that end have international legal personality, that is, they have their rights and obligations under international law.[56] The practice of international organizations in international relations (when accompanied by opinio juris) may count as a practice that gives rise to or attests to rules of customary international law. However, this is limited to those rules (a) whose subject matter falls within the mandate of the organizations, and/or (b) that are addressed specifically to them (such as those on their international responsibility or relating to treaties to which international organizations may be parties).[57]

In the cyberspace area, the development of technology also triggered a new methodical approach in warfare, this also a special condition that has similarities with the development of space law by state practices along with contributions from international organizations. The cyber-attack in Estonia raised a new concern and urged NATO and European Network and Information Security Agency (ENISA) to take a further step in preventing and improving cyber-defense. In November 2011 in Lisbon, NATO adopted a new strategic approach to simulate cyber- defense in a multinational dimension along with other European Union states.[58] Tallinn Manual 1.0 emerged from states' concerns about cyber- attack that

---

51 *Ibid.,* at 66 – 68.

52 Sevis, Kamile Nur, and Ensar Seker. "Cyber warfare: terms, issues, laws and controversies." *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, 2016, pp. 1-9.

53 *Ibid.,* at 4.

54 *Ibid.*

55 *Supra note* 30, at 130.

56 *Ibid.*

57 *Ibid.*

58 Herzog, *supra note* 3, at 55.

occurred in many events, such as 9/11 WTC, cyber-attack in Estonia, cyber-attack in Georgia, Stuxnet cases in Iran, etc. that were initiated by CCD COE NATO.[59] Likewise, the general practices in space law, the length of the practices is not a key-factor to prove the existence of general practice since both of the matters happened very quickly due to the rapid development of technology.

Surely the formation and validation of general practice initiated by states and international organizations could not be compared equally since they have different legal personalities and legal capacities as subjects of international law. However, such conduct may have an indirect role in the identification of customary international law, by stimulating or recording the practice and acceptance as law (opinio juris) of States and international organizations.[60] In IHL, the International Committee of the Red Cross (ICRC) plays an important role in shaping the practices of the state, such as appeals for and memorandums on respect for international humanitarian law or their publications regarding identifying relevant practice.[61] It can be concluded that cyber-attack in times of armed conflict has been generally practiced not only by states but also by international organizations.

2. The Element of Opinio Juris

Opinio juris sive necessitatis commonly known as opinio juris, is a belief that state practice is legally mandatory and it became a factor that changes state practice to be customary international law.[62] Opinio juris is a subjective element in customary international law and can be a bit tricky since not every state expresses its consent about a certain general practice explicitly. An implicit consent might be given by a state to the international community, commonly known as a tacit agreement.[63] Yet tacit agreement is also quite tricky to determine an opinio juris element. As ICJ once said, "acting, or agreeing to act in a certain way, does not of itself demonstrate anything of a juridical nature".[64] Following the ICJ's statement, to examine an opinio juris has never that simple, the agreeing act has to reflect a juridical nature and obligatory. However, this element is still vital to show the establishment of customary international law.

According to ILC, there are two requirements of opinio juris to be accepted as a law:[65]

1. The requirement, as a constituent element of customary international law, that the general practice is accepted as law (opinio juris) means that the practice in question must be undertaken with a sense of legal right or obligation.
2. A general practice that is accepted as law (opinio juris) is to be distinguished from mere usage or habit.

Considering the first requirement of opinio juris as an acceptance of law, the acceptance could be expressed explicitly and firmly by representatives of the states. This is expressed explicitly by some high-influencing states. The Netherlands announces their agreement of cyber-attack in International Humanitarian Law by a letter from the Ministry of Foreign Affairs to their parliament.[66]

"It re-affirms that the

59 Schmitt, *supra note* 1, at 16.
60 *Supra note* 30, at 132.
61 *Ibid.*
62 Shaw, *supra note* 29, at 84.
63 Slouka, Zdenek J. *International custom and the continental shelf: a study in the dynamics of customary rules of international law*. Netherlands: Springer, 2012.
64 *Supra note* 30, at 129.
65 *Ibid.,* at 138.
66 UN GGE, "The Netherlands position on International Law in Cyberspace made public", https://dig.watch/updates/netherlands-position-

> *international humanitarian law, as well as neutrality law, applies to cyber-operations conducted during armed conflict, as well as that the international human rights laws apply to cyberspace, though it acknowledges that human rights are not absolute and sometimes lawfully may be limited (with legitimacy and proportionality take into consideration). In the context of self- defense, retorsion, as well as both cyber and non-cyber countermeasures are allowed responses to cyber-attacks, necessity plea applies in case of attacks against critical infrastructure, and when there are potentially very serious consequences at stake, while self - defense may include a response by all means in case of a cyber "armed attack" (where cyber-operation may be characterized as "armed attack" if, in terms of scale and effects, it represents the gravest form of use of force)".*

The letter said that cyber-attack must apply equally in International Humanitarian Law whether in offense or defense and can make massive impacts, it is solid proof of the Netherland's position and its *opinio juris* on this issue.

Following the Netherlands, the United Kingdom also announces it by its Attorney General, Jeremy Wright.[67] Jeremy Wright referred to three articles in the UN Charter, which are: Article 2 (4) about use of force, Article 2 (7) about the prohibition of intervention in domestic affairs; and Article 51 about self- defense, according to Jeremy Wright, all of them have to be applied equally in cyber-space.[68] France also agreed with cyber-attack practice in International Humanitarian Law its Ministry of Armies stated France's position and perspective on the matter of cyber-attack.[69] France also agreed that cyber-operations launched because of hostility and enmity to France's cyber-infrastructure or gave any impact to France's territory and threatening sovereignty as an internationally wrongful act.[70] France added, this applied whether the cyber-attack was done by a state organ, person, or entity aligned with Articles 4, 5, and 8 of the 2001 Article of State Responsibility of International Wrongful Act.[71]

The United States also announced its position and agreement about this matter represented by Harold Koh, Legal Advisor in the U.S. Department of State.[72] Harold Koh confirmed that the United States agreed to enact just ad bellum by use of force in cyberspace, as long as those attacks can give equal impacts as conventional or kinetic attacks.[73] He also added by using a bomb analogy which could ruin and damage a water dam and flooding its surrounding, this impact could happen because of a malware which attacks the system and damages the water dam.[74] Michael N. Schmitt responds to all of the statements, those statements are a progressive development of *opinio juris*

---

international-law-cyberspace-made-public. Accessed on 17th of April 2020.

67 Wright, Jeremy, "Cyber and International Law in the 21st Century", 23rd May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century. Accessed on 19th of October 2020.

68 *Ibid.*

69 Schmitt, Michael N., "France's Major Statement on International Law and Cyber: An Assessment", *Just Security, https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.* Accessed on 19th of October 2020.

70 *Ibid.*

71 *Ibid.*

72 Koh, Harold Hongju, "International Law in Cyberspace", *USCYBERCOM Inter-Agency Legal Conference,* stated on 18th September2012, https://20092017.state.gov/s/l/releases/remarks/197924.htm. Accessed on 19th of October 2020.

73 *Ibid.*

74 *Ibid.*

to emerge a customary international law.[75]

Following the second requirement of the law acceptance in opinio juris, without consent from the states, general practice is considered themselves legally free either to follow or to disregard does not contribute to or reflect customary international law (unless the rule to be identified itself provides for such a choice).[76] The consent from a state is therefore mandatory to legalize a new norm in international law. State objection to a certain general practice shows that the state disagrees with that certain rule. The objection towards the general practice of cyber-attack under international humanitarian law had been declared by Russia.

In precise, Russia has declined military practice in cyber-space under International Humanitarian Law. Konstantin Peschanenko is a spokesperson from Russia's Ministry of Defense supported by Andrei Krutskikh as Roving Ambassador stated that Russia prevents military activities in cyberspace.[77] Russia's objection may be questionable, whether this practice can be enforced as customary international law or not considering Russia's objection will be a failing opinio juris.

However, Russia's objection could not be classified as a persistent objector. International Law of Association (ILA) defined persistent objector by referring to the committee report of Formation of Customary (General) International Law, that said: 'if there's a general practice is developing to customary international law, then if there is a state who consistently has a different opinion and position with that practice than the state will not be binding to it'.[78] In addition, according to ILC, a persistent objector is:[79]

1. Where a State has objected to a rule of customary international law while that rule was in the process of formation, the rule is not opposable to the State concerned for so long as it maintains its objection.
2. The objection must be clearly expressed, made known to other States, and maintained persistently.
3. The present draft conclusion is without prejudice to any question concerning peremptory norms of general international law (jus cogens).

The objection has to be clearly expressed, by stating a clear verbal objection, either in written or oral form, as opposed to physical action, which will suffice to preserve the legal position of the objecting State.[80] Besides, the objection must have been made while the rule in question was in the process of formation.[81] Even though Russia had objected to this in the middle of the establishment of customary international law, yet Russia's act was contradictive with its objection since Russia had attacked Estonia and Georgia by using cyber-weapon. It means that Russia's objection is merely a political stand to this matter to avoid responsibilities or other consequences.

---

75 Schmitt, Michael N. "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis", *Just Security,* https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/. Accessed on 19th of October 2020.

76 *Supra note* 30, at 140.

77 Vlast, Kommersant and Elena Chernenko, "Russia Warns Against Nato Document Legitimizing Cyberwars", https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html, accessed on April 16th 2020

78 Green, James A. *The persistent objector rule in international law*. Oxford: Oxford University Press, 2016.

79 *Supra note* 30, at 152.

80 *Ibid.,* at 153.

81 *Ibid.*

However, Antonio Cassese also added that there is no international judgment to support this doctrine's existence.[82]

Both elements of customary international law had existed in the emerging norm of Rule 30 Tallinn Manual 1.0. The establishment of Tallinn manual 1.0 by NATO and other states had urged and pushed the international community to put more attention to this matter. Along with the state's practices that had been established before and after the Tallinn Manual 1.0 drafted and opinio juris from some high-influencing states to support the emerging norm from Rule 30 of Tallinn Manual 1.0. However, it is argued that both elements are still insufficient to validate Rule 30 of Tallinn Manual 1.0 as a new customary international law. This article, therefore, provides another theory in the following section to strengthen its argument that Rule 30 of Tallinn Manual 1.0 has fulfilled the customary nature.

D. GROTIAN MOMENT THEORY: INSTANT CUSTOMARY INTERNATIONAL LAW IN RULE 30 TALLINN MANUAL 1.0

Richard Falk introduced a Grotian Moment Theory in 1985 as a term to explain the development and shifting paradigm when there is a new rule and new norm existed and quickly accepted by the international community with unusual pace acceptance.[83] This theory also defines as a parable of fundamental change at the end of an ongoing international system, then triggers the existence of a new principle from customary quick acceptance by the international community'.[84] According to this theory, situations that can be classified as a fundamental change are such as the development of technology; a massive historical event; and many more, these changes can push the establishment of customary international law. This statement also supported by Max Planck in Encyclopedia of Public International Law as follows:[85]

> *"This can be due to the urgency of coping with new developments of technology, such as, for instance, drilling technology as regards the rules on the continental shelf, or space technology as regards the rule on the freedom of extra-atmospheric space. Or it may be due to the urgency of coping with widespread sentiments of moral outrage regarding crimes committed in conflicts such as those in Rwanda and Yugoslavia that brought about the rapid formation of a set of customary rules concerning crimes committed in internal conflicts."*

It is worth considering the opinion from Cheng regarding the difference between the Grotian moment theory from the formation or emergence of instant customary international law. According to Cheng, an opinio juris is sufficient to validate the emergence of instant customary international law.[86] In other words, the element of general practice is not vital and important in emerging a customary international law. This theory undoubtedly brings a polemic in international law since the Grotian Moment theory does not focus on one of the customary international elements. It rather requires both elements of customary international law to be satisfied.

According to Michael P. Scharf, this

---

82 *Ibid.,* at 45.

83 Sterio, Milena. "Humanitarian Intervention Post-Syria: A Grotian Moment." *ILSA Journal of International & Comparative Law,* vol. 20, no. 2, 2014, pp. 343-356, at 343.

84 *Ibid.,* at 343.

85 Scharf, Michael P. "Accelerated formation of customary international law." *ILSA Journal of International & Comparative Law,* vol. 20, no. 2, 2014, pp. 306-342, at 305.

86 Hoof, *supra note* 28, at 175.

theory emerged and existed in Nuremberg Tribunal, with the emergence of a new paradigm that a person can be considered as an international law subject in terms of bearing responsibility.[87] This new paradigm then shifted into a new principle and was adopted by the International Law Commission (ILC) that the Nuremberg Charter and Nuremberg Tribunal have established a new rule that is the individual responsibility of criminal act.[88] Before Nuremberg, the only subjects of international law were States, and what a State did to its citizens within its borders was its own business.[89] This new principle then became a fundamental shifting and development of international criminal law. Supported by the ICJ statement, the European Court of Human Rights and four other International Criminal Court (ICC) also confirmed this principle and affirmed that Nuremberg Tribunal Judgment and Charter as customary international law.[90]

Furthermore, on December 11, 1946, in one of the first actions of the newly formed U.N., the General Assembly unanimously affirmed the principles from the Nuremberg Charter and judgments in Resolution 95 (I).[91] This General Assembly Resolution had all the attributes of a resolution entitled to great weight as a declaration of customary international law: It was labeled an "affirmation" of legal principles; it dealt with inherently legal questions; it was passed by a unanimous vote, and none of the members expressed the position that it was merely a political statement.[92] This occurred event reflects that a massive historical moment can shift the old international law paradigm and enforce a new norm to adapt to an alteration, this key is the point that distinguishes the difference between the Grotian moment theory and the instant customary international law by Cheng. Also, the Grotian moment theory contemplates the accelerated formation of customary international law through widespread acquiescence or endorsement in response to State acts, rather than instant custom based solely on General Assembly resolutions.[93] The Grotian Moment theory may rely on General Assembly resolutions to discover evidence of an emerging customary law norm, resulting from a period of fundamental change.[94] However, General Assembly resolutions are one of the many tools utilized by scholars discovering a Grotian Moment.[95]

Moreover, the alteration of technology also can shift the paradigm of international law. This can be seen for the first time in a matter of continental shelf limitation started by the United States. By using the Truman Proclamation in 1945, the United States was the only state who had the capacity and advanced technology, so that they took initiative to set a continental shelf.[96] In 1969, ICJ confirmed Truman Proclamation as customary international law and legally binding to all states with or without they had ratified the Convention of the Sea 1958,[97] as well as the fast-paced technology development in space exploration led by the United States and Uni Soviet (Russia) until it became customary international law and legally binding to all states. Besides, many scholars concluded that the General Assembly Declaration in 1963 was representing an authoritative statement that customary international law can quickly establish to respond to the fast-paced technology development and shifting international law paradigm.[98]

According to the preceding paragraphs, it can be concluded that The Grotian Moment Theory could also be used as a basic theory to validate the Rule 30 Tallinn Manual 1.0 as customary international law.

87 Scharf, *supra note* 86, at 330 – 332.
88 *Ibid.,* at 332.
89 *Ibid.*
90 *Ibid.,* at 334.
91 *Ibid.,* at 333.
92 *Ibid.*
93 Sterio, *supra note* 84, at 345.
94 *Ibid.*
95 *Ibid.*
96 Scharf, *supra* note 86, at 335.
97 *Ibid.*
98 *Ibid.,* at 336.

In terms of rapid technology development, cyber-attack has similarity with space customary international law that the existing law needs to adapt with the alteration that occurred. The cyber-attack that happened in Estonia had similarities with Nuremberg Tribunal since it was the first cyber-attack that happened in history which was completely done in cyber-space, yet it gave equal impacts as a conventional or kinetic attack. This incident attracted and concerned many states and gave new urgency to the international community to take serious action in responding to the cyber-attack issue. It is therefore sufficient to conclude that the Grotian Moment Theory provides a basis for the emergence of the customary nature of Rule 30. This establishment of a new customary international law will give the international community a legal certainty about the threshold of cyber-attack to trigger the applicability of IHL.

E. CONCLUSION

The cyber-attack in Estonia in 2007 has urged the international community to provide more specific rules concerning the use of cyberweapons in international law, particularly in IHL. This is because the existing IHL rules are not sufficient to answer the problem of its applicability in the case of cyber-attack employed alone without being accompanied by other kinetic weapons but has caused severe physical impacts that are equal to the kinetic one. Rule 30 of Tallinn Manual 1.0 provides a clear threshold in this regard, however, it cannot be used as a legal basis due to its soft-law nature.

This article has provided evidence that Rule 30 of Tallinn Manual 1.0 met both elements of customary international law, that is general practices and opinio juris, even though it is not in its ideal condition. Likewise space customary international law that has emerged due to the rapid technology development, Rule 30 Tallinn Manual also has similar reasons to be emerged. This provision plays a significant role in protecting human beings from non-kinetic attacks that were designed due to the development of technology. IHL can protect the civilian by limiting and prohibiting certain weapons that may cause unnecessary suffering including the employment of cyber weapons. It is therefore necessary for IHL to apply in cyber-attack situations for as long as the threshold of the existence of armed conflict has been met.

In the effort to provide a more convincing argument that Rule 30 is sufficient to be considered as customary international law, this article refers to the Grotian Moment Theory that in practice has successfully proven the space law as well as individual criminal responsibility as instant customary international law rules. Both space law and individual criminal responsibility emerged due to the fundamental change of the situation in the world that needed an urgent response from the international community. The rapid technology development and their important role to protect human beings as well as to provide legal certainty for the international community are sufficient reasons for Grotian Moment Theory to accelerate one rule as a customary rule since they meet the fundamental change element.

REFERENCE

Books

Boothby, William H. *Weapons and the law of armed conflict*. Oxford: Oxford University Press, 2016.

Green, James A. *The persistent objector rule in international law*. Oxford: Oxford University Press, 2016.

Hoof, GJH Van. *Pemikiran Kembali Sumber-Sumber Hukum Internasional*. Bandung: Yayasan Obor Indonesia, 2000.

Schmitt, Michael N. (ed). *Tallinn Manual 1.0 on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press, 2013.

Shaw, Malcolm N. *International law.* Cambridge: Cambridge University Press, 2017.

Slouka, Zdenek J. *International custom and the continental shelf: a study in the dynamics of customary rules of international law*. Netherlands: Springer, 2012.

Tikk, Eneken, (*et.al.)*. *International cyber incidents: Legal considerations*. Estonia: Cooperative Cyber Defence Centre of Excellence, 2010.

Journals

Grignon, Julia. "The beginning of application of international humanitarian law: A discussion of a few challenges." *International Review of the Red Cross*, vol. 96, no. 893, 2014, pp. 139-162.

Herzog, Stephen. "Revisiting the Estonian cyber-attacks: Digital threats and multinational responses." *Journal of Strategic Security,* vol. 4, no.2, 2011, pp. 49-60.

Jensen, Eric Talbot. "The Tallinn Manual 2.0: Highlights and Insights." *Georgetown Journal of International Law,* vol. 48, 2017, pp. 735-778.

Khatwani, Naman. "Common Heritage of Mankind for Outer Space." *Astropolitics,* vol. 17, no. 2, 2019, pp. 89-103.

Pellet, Allain, "Article 38", *Commentary: The Statute of the International Court of Justice*, edited by Andreas Zimmermann (*et.al*.), Oxford University Press, 2012, pp. 676 -793.

Scharf, Michael P. "Accelerated formation of customary international law." *ILSA Journal of International & Comparative Law,* vol. 20, no. 2, 2014, pp. 306-342.

Schimdt, Andreas. "The Estonian Cyber Attacks". *The Fierce Domain Conflicts in Cyberspace 1986-2012*, edited by Jason Healey. Atlantic Council, 2013, pp. 174 -193.

Sterio, Milena. "Humanitarian Intervention Post-Syria: A Grotian Moment." *ILSA Journal of International & Comparative Law,* vol. 20, no. 2, 2013, pp. 343-356.

Yapici, Merve İrem. "What Role Did Nashi Play in Russian Internal Politics and Foreign Policy: A Formulator or an Implementer." *Review of International Law and Politics,* vol. 12, no. 2, 2016, pp. 101-137.

Other Documents

Kagan, Kimberly. "Iran's Proxy War Against the U.S and the Iraqi Government". *Institute for the Study of War and weeklystandard.com,* Mei 2006 – 20 August 2007. http://www.understandingwar.org/report/irans-proxy-war-against-united-states-and-iraq.

Koh, Harold Hongju, "International Law in Cyberspace", *USCYBERCOM Inter-Agency Legal Conference,* stated on 18th September 2012, https://20092017.state.gov/s/l/releases/remarks/197924.htm.

Ku, Julian, "Defining the Customary International Law of Outer Space", http://opiniojuris.org/2006/10/18/defining-the-customary-international-law-of-outer-space/.

Oxford English Dictionary (OED), https://www.oxfordlearnersdictionar

ies.com/definitio n/english/cyber?q=cyber.

Oxford English Dictionary (OED), https://www.oxfordlearnersdictionaries.com/definitio n/english/operation?q=operation.

Parker, Diantha (*et.al*.). "Iran, the United States and the Political Seesaw", *The New York Times*,https://archive.nytimes.com/www.nytimes.com/interactive/2012/04/07/world/middleeast/irantimeline.html #/#time5_211.

Schmitt, Michael N. "The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis", *Just Security,* https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/.

Schmitt, Michael N., "France's Major Statement on International Law and Cyber: An Assessment", *Just Security, https://www.justsecurity.org/66194/frances-major-statement-on-international-law-and-cyber-an-assessment/.*

Sevis, Kamile Nur, and Ensar Seker. "Cyber warfare: terms, issues, laws and controversies." *2016 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, 2016, pp. 1-9.

UN GGE, "The Netherlands position on International Law in Cyberspace made public", https://dig.watch/updates/netherlands-position-international-law-cyberspace-made-public.

Vlast, Kommersant and Elena Chernenko, "Russia Warns Against Nato Document Legitimizing Cyberwars", https://www.rbth.com/international/2013/05/29/russia_warns_against_nato_document_legitimizing_cyberwars_26483.html

Wright, Jeremy, "Cyber and International Law in the 21st Century", May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century.

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

Legal Documents

Commentary Konvensi Jenewa I 1949, 2016, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=BE2D518CF5DE54EAC1257F7D0036B518#_Toc452041593

Commentary Protokol Tambahan I 1977, 1987, https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=7125D4CBD57A70DDC12563CD0042F793

Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Prosecutor V. Dusko Tadic A/K/A "Dule", Case No. IT-94-1-T, 2nd October 1995

Draft Conclusions on Identification of Customary International Law with Commentaries, adopted by the International Law Commission and submitted to the General Assembly (A/73/10), 2018.

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 12 August 1949 (Geneva Convention I 1949)