Available online at: http://jurnal.uns.ac.id
Yustisia Jurnal Hukum
| ISSN (Print) 0852-0941 | ISSN (Online) 2549-0907 |
YUSTISIA Yustisia Jurnal Hukum

Cyber-Attack in Estonia: a New Challenge in The Applicability of International Humanitarian Law

Iradhati Zahra[1]; Irawati Handayani[2]; Diajeng Wulan Christianti[3]
[1]Student in Bachelor Degree at Faculty of Law, University of Padjadjaran
[2,3]Lecturer at Faculty of Law, University Padjadjaran
Corresponding author's email: iradhatizahra@gmail.com

Article Information

Submitted : 04 February 2021
Reviewed : 04 March 2021
Accepted : 30 March 2021

Keywords:
application of international humanitarian law; Estonia's cyber-attack; armed conflict

DoI: 10.20961/yustisia.v10i1.48336

Abstract

This article aimed to analyze the classification of armed conflict in Estonia's cyber-attack and how the existing IHL are answering this problem, and whether those regulations are enough for future cases of cyber-attack. This article uses the normative method by comparing the Geneva Convention 1949 and Additional Protocol I 1977 with Rule 30 Tallinn Manual 1.0 and some relevant literary works, using a descriptive-analytic to explain the object comprehensively. The result shows that Estonia's cyber-attack could be classified as an International Armed Conflict, which first started as a Non-International Armed Conflict by proving attribution from Russia to Nashi Youth Group following the Overall Control in Tadic Case. The distinction between information warfare and cyber-attack is related to the physical impact, which a threshold of a cyber-attack under Tallinn Manual 1.0. It means Rule 30 of Tallinn Manual 1.0 also answered Jus ad Bellum's threshold and Jus in Bello in terms of cyber-attack. Although, this article needs some improvements regarding the limitation of this issue only focused on the Material Scope of IHL. In addition, Rule 30 of Tallinn Manual 1.0 is not legally binding because it is not one source of international law. However, it is possible for the Rule 30 Tallinn Manual 1.0 to be a new norm and becoming customary international law in the future.

I. Introduction

The industry revolution 4.0 brings a fast-paced change in various fields, including the implementation of cyber-weapon in International Humanitarian Law (IHL). The utilization of cyber is not new to current practice in IHL, yet this matter's regulation is not fully established. It does not give legal certainty to international communities. One of the concerning issues is regarding launching a cyber-attack on the enemy. A cyber-

attack attempts to gain illegal access to a computer or computer system to cause damage or harm (Merriam-Webster Dictionary, 2020).

The polemic of cyber-attack might intersect with the use of force, as a Jus ad Bellum, in Article 2 (4) UN Charter, the definition of cyber-attack should be differentiated with aggression as an act of use of force. The General Assembly Resolution No. 3314 define aggression without including cyber-attacks as one of the limitations because the resolution itself was published in 1974, meanwhile, Rule 30 of Tallinn Manual 1.0 gives a limitation of how a cyber-attack could be classified as a Jus in Bello or to trigger the beginning application of IHL. However, the definition of aggression under GA Resolution No. 3314 and the understanding of cyber-attack is quite tricky to solve because there are requirements of a cyber-attack to be a trigger the beginning application of IHL, they are the non-kinetic character and the physical impacts. There requirements will differentiate the Jus ad Bellum and Jus in Bello in the case of cyber-attack.

As this happened in Estonia in 2007, a cyber-attack had launched and gave impactful massive damage to Estonia (Herzog, 2011). This case started on April 30, 2007, when the Estonian government moved a copper soldier statute – a memorial of Uni Soviet effort to liberating Estonia from Nazi – from Tõnismägi Park downtown Tallinn Military Cemetery in the outskirt of Tallinn (Herzog, 2011). This movement of the statue triggered tension between the Estonian Civilians and the Russian Minorities. For the Estonian Civilians, the statue represents Russia's oppression of Estonia, and for the Russian Minorities, the movement of the statue to the outskirt of Tallinn represents a marginalization of their ethnic (Herzog, 2011). The tension then followed by a massive protest in front of Estonia's Ambassador in Russia by Nashi Youth Group and a cyber-attack launched by Sergei Markov and Konstantin Goloskokov, *Commissars* in Nashi Youth Group, along with their followers (Herzog, 2011).

Followed by the statue movement and Nashi Youth Group's xenophobic atmosphere, the cyber-attack was launched using Distributed-Denial of Service (DDoS). The attack deliberately targeted a website or an application to make it unavailable to users, such as by flooding it with network traffic (Amazon Web Services, 2019). The cyber-attack was started structured very well. On April 27, 2007, by targeting some essential websites such as the president's website, Estonia's parliamentary, Estonia's Police, Political Parties, and highly influencing mass media (NATO, n.d.). Also, the parliamentary email was disabled because of the cyber-attack. On May 4, 2007, the cyber-attack targeted banking sectors in a more coordinative way than before, such as Hansa Bank and SEB Eesti Uhisbank and failing the Automatic Teller Machine (ATM) and make them a loss of 1.000.000 $USD (NATO, n.d.). Later the cyber-attack culminated on May 9, 2007, along with the Russian Federation's Independence Day to commemorate their winning over Nazis in the Great Patriotic War (NATO, n.d.).

Besides the previous damages, the cyber-attack also affected some of Estonia's infrastructures, such as damaging Tallinn's water supply, which was necessary for civilians in Tallinn City (Herzog, 2011), and cut off commercial transportation in Tallinn (NATO, n.d.). The cyber-attack was also done by humiliating the Prime Minister of Estonia, Andrus Ansip Pidor, with rude words (Herzog, 2011). The cyber-attack was suddenly and simultaneously stopped on May 19, 2007 (Schmidt, 2013). Several months

after the cyber-attack, Sergei Markov and Konstantin Goloskokov admitted their attack. They claimed that they were the perpetrator of the cyber-attack and no involvement of the Nashi Youth Group nor the Russian Government (Herzog, 2011). On the other hand, some of the outsider or the third party's statements stated that there was Russia's involvement in the cyber-attack, along with some facts about the Government's Control over the Nashi Youth Group.

Besides the cyber-attack in Estonia, there were two cyber-attack cases that had happened, namely Georgia v. Russia in 2008 and Stuxnet in Iran, which perpetrated by the United States and Israel (Kimberly Kagan, 2007; Tikk, 2010; Zetter, 2014). However, those two cases have a significant difference from the Case of Estonia. The cyber-attack in Estonia ultimately launched in cyber-space with massive damages compatible with a conventional attack. On the other hand, the cyber-attack in Georgia v. Russia and Stuxnet in Iran happened after the conventional attack was launched.

The difference in the main problem in IHL nowadays is that in practice, IHL applies if the hostilities followed by an attack give an injury to a person or death to a person or damage to an object. The attack and the impact were always apparent enough in the current practice of IHL. This weapon shoots at a person and causes injury or death can apply the beginning application of IHL without a doubt. Meanwhile, the cyber-attack was a particular case. A cyber-attack could not be seen or perceived immediately. It does not have any kinetical movement, just like a conventional attack, yet the impact can be harmful both physically and non-physical way. The Commentary 2016 on Common Article 2 Geneva Convention 1949 had tried to solve the problem, yet the commentary is still not clear and firm in determining how far a cyber-attack could trigger the beginning application of IHL.

Following that event, in 2013, CCD COE NATO established a manual about cyber-warfare along with other scholars and practitioners, the manual called *Tallinn Manual 1.0 on the International Law Applicable to Cyber-Warfare* (Tallinn Manual 1.0). The document discussed how cyber-warfare should apply under IHL comprehensively, also Rule 30 of Tallinn Manual 1.0 had achieved set a threshold for a cyber-attack in triggering the beginning application of IHL. However, Tallinn Manual 1.0 is not a source of international law according to Article 38 ICJ Statute.

This article will start with three sections, the first section will begin with determining the classification of armed conflict in the cyber-attack in Estonia. Authors use attribution to prove the relation between Russia and Nashi Youth Group and classified it as IAC. Following the status of armed conflict as an IAC, the second section will analyze how the existing IHL (Common Article 2 Geneva Convention 1949 and Article 49 (1) Additional Protocol I 1977) are answering this problem, and whether those regulations are enough for the future cases of cyber-attack. After analyzing the existing regulations of IHL, the last section in this article will take a look at Rule 30 Tallinn Manual 1.0 and break down the element in Rule 30 of Tallinn Manual 1.0 to see its compatibility to IHL.

Comparing this article with published articles from some authors, the novelty of this article is this article uses the cyber-attack in Estonia as an object and focus of the discussion. Ido Kilovaty in his article titled "Cyber Warfare and the *Jus ad Bellum*

Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare", also discussed this issue along with the attribution approach in his paper. However, his article is more general and did not specifically bring the cyber-attack in Estonia as the main object, as well as the attribution approach which did not elaborate on each of the cyber-attack cases. The article titled "Applying International Humanitarian Law to Cyber Warfare" by Eitan Diamond also discussed the beginning application of IHL in its article, but this article focused on what kind of circumstance of cyber operations could trigger the beginning application of IHL along with the principles of warfare (distinction, proportionality, precautions, etc.), and this article did not bring the cyber-attack in Estonia as the main object of the article. Inspired by those articles, the authors bring this topic with a more specific object (the cyber-attack in Estonia) to be elaborated and analyze as a novelty of this article.

II. Classification of Armed Conflict in the Case of Estonia

Considering Nashi Youth Group's relationship with the Russian government, the raising question is whether this case can be classified as an IAC with Russia as the actual perpetrator of the cyber-attack. The first thing is to see whether there is a state attribution from Russia to Nashi Youth Group to prove their relationship. According to Article 8 (Draft Articles of State for Internationally Wrongful Acts (ARSIWA), *"The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is acting on the instructions of, or under the direction or control of, that State in carrying out the conduct"*(Walter et al., 2004). This article explains the relevance of Nashi Youth Group's position in Russia since Nashi Youth Group is not a state organ and does not have any authority to exercise the government's control according to Articles 4 and 5 of ARSIWA.

Article 8 of ARSIWA contains two thresholds of control from a state to a person of an entity. The thresholds are Effective Control and Overall Control. Overall control was established from Tadic Case with ICTY's interpretation over Article 8 ARSIWA. Meanwhile, Effective Control was applied to Paramilitary Activity in Nicaragua (Nicaragua v. the USA) and Genocide in Bosnia (Walter et al., 2004). There are three significant distinctions between Effective Control and Overall Control, but considering the cyber-attack was perpetrated by the Nashi Youth Group, there is an escalation of armed conflict from NIAC to IAC, or as we can see as an internationalized armed conflict, This is not a legal terminology, yet it refers to NIAC who have IAC characteristics. In IHL, this situation might end up as IAC, NIAC, or both of them (it depends on the nature of the parties). In this case, this armed conflict is IAC which was started by NIAC (Sassoli, n.d.).

A. Fulfillment of NIAC

According to the Judges of ICTY in para. 562, Tadic Case had fulfilled a classification to be NIAC (*Opinion and Judgement on Prosecutor v. Dusko Tadic A/K/A "Dule,"* 1997). Referring to the Tadic Case, a classification to be NIAC is essential to prove whether there is an internationalized armed conflict or not. Common Article 3

Geneva Convention 1949 and Article 1 Additional Protocol II 1977 regulated that two thresholds must be fulfilled to be classified as NIAC, namely the level of organized armed groups and intensity of the conflict.

First, Nashi Youth Group had fulfilled the threshold to be an organized armed group. As we can see from their vision and purposes of establishment, this organization has a clear vision and methods to execute its goals (YAPICI, 2016). Also, this organization has a clear organizational structure from a supreme leader (Vasily Yakemenko), Commissar (two of them are Sergei Markov and Konstantin Goloskokov), and other members under them (YAPICI, 2016). It explains that, as an organized armed group, Nashi Youth Group has fulfilled an organized group's characteristics.

As for whether the group was armed, the Nashi Youth Group is weaponed with cyber-weapon, and the cyber-weapon itself had been used to attack Estonia in 2007 and *Kommersant* in 2008 (Atwal, 2012). According to *The Manual on the Law of Air and Missile Warfare* (AMW Manual), defines 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*"(HPCR, 2009). This definition fits with cyber as a weapon in Estonia and Kommersant cases since this definition emphasizes weapons from their impact on persons and objects. It means that a cyber-weapon can be considered a weapon according to that definition. In conclusion, the Nashi Youth Group can be classified as an organized armed group, with clear structures and purposes along with their cyber-weapon to execute their missions.

Second, the intensity of conflict must be high to be classified as NIAC. According to Marco Sassoli and D. Schindler, how a state is handling and responding to the attack reflecting the intensity of the conflict, for example, by moving armed forces or police to see how severe the attack was (ICRC, 2008). In cyber-attacks in Estonia, Estonia couldn't solve and defend its country by itself. NATO and *European Network and Information Security Agency* (ENISA) lend them a hand to launched cyber-attacks as a defense (Herzog, 2011). Estonia could not handle the cyber-attacks by themselves proved that the intensity was severe and harmful, so it is logical to conclude it as NIAC since the intensity was intense.

Therefore, the Estonia cyber-attacks were enough to be classified as NIAC since Nashi Youth Group is proved to be an organized armed group. The intensity of the cyber-attacks was intense and harmful to Estonia.

B. Fulfillment of IAC

1. Comparison Between Effective Control and Overall Control

Following the fact that the cyber-attack in Estonia has fulfilled classification to be NIAC, the next step is to prove state attribution from Russia to Nashi Youth Group. As mentioned before, there are two types of Control in Article 8 ARSIWA, namely Effective Control and Overall Control. There are three distinctions between Effective Control and Overall Control explain why Effective Control has a higher threshold than Overall Control.

First, Effective Control required a specific instruction or direction to execute the state command (Walter et al., 2004). Referring to the Bosnian Genocide Case, the ICJ judges found that Yugoslavia had done its job to prevent the genocide. Therefore they could not be asked for state responsibility (Marttinen, 2016). Also, in Nicaragua v. the USA, there was no evidence that the USA gives specific instruction to the perpetrator, even though the United States has been proven to fully support them by equipping, financing, training, etc. (Walter et al., 2004). Therefore, both cases have not fulfilled the 'specific instruction,' and the attribution is not enough to demand state responsibility. Meanwhile, the Overall Control in Tadic Case didn't require 'specific instruction' to legitimize state attribution (Cassese, 2007). In Tadic Case, the Judges of ICTY interpreted that an Overall Control should be enough to legitimize state attribution from Yugoslavia to Bosnian Serbs because of Nicaragua v. the USA Bosnian Genocide, the attribution in Tadic Case had a different purpose with them (Walter et al., 2004).

Second, Effective Control and Overall Control were applied in a different judicial body. The Nicaragua v. USA and Bosnian Genocide were trialed by the International Court of Justice (ICJ) with jurisdiction over state parties according to Article 34 ICJ Statute (Only states may be parties in cases before the Court). Meanwhile, following Article 6 of the International Court of Tribunal for Yugoslavia (ICTY), they had jurisdiction over the individual as a subject of international law (The International Tribunal shall have jurisdiction over natural persons pursuant to the provisions of the present Statute). It means that the attribution in Tadic Case could not be asked for state responsibility. Still, it was only to prove the relation between Yugoslavia (FRY) and Bosnian Serbs. Otherwise, the attribution in Nicaragua v. the USA and Bosnian Genocide were meant to be asked for state responsibilities (Walter et al., 2004).

Third, Effective Control and Overall Control have a different purpose and subject matter. According to the Judges of ICTY's interpretation, the attribution in Article 8 ARSIWA was used to escalate the armed conflict from NIAC to IAC since, in Article 2 of ICTY, the statute only applies to IAC (*Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Prosecutor V.Dusko Tadic A/K/A "Dule,"* 1995). The ICTY Judges interpreted Article 8 of ARSIWA to prove the attribution between Yugoslavia to Bosnian Serbs from that urgency. Therefore, the armed conflict could be escalated as IAC and under ICTY's jurisdiction. On the other hand, Nicaragua v. the USA and Bosnian Genocide's attribution was meant to asked state responsibilities to align with ICJ's jurisdiction over state disputes (Walter et al., 2004).

Therefore, from those three, the Effective Control requires a specific instruction and Overall Control to prove attribution from a state to perpetrator so that the state responsibilities could be asked. The Overall Control does not require a particular instruction from the state to the perpetrator. It means the Overall Control has a lower threshold than Effective Control.

2. Requirements of Overall Control

Following the previous comparison, the cyber-attack in Estonia has a similar situation with Tadic Case, and therefore the Overall Control applies to Estonia's case. According to the Commentary of Article 8 ARSIWA and referring to the Tadic Case, five requirements have to be fulfilled to be defined as Overall Control, namely: Organized Armed Group, Financing, Supervising, Planning, and Equipping (Walter et al., 2004).

First, as explained earlier, Nashi Youth Group as a perpetrator of the attack has fulfilled thresholds to be an Organized Armed Group, with their organizational structure and cyber-weapon (Herzog, 2011; Schmidt, 2013). Vasily Yakemenko is both responsible as a supreme leader for Nashi Youth Group and founder of Nashi Youth Group since 2005 (Atwal, 2012). He is also a highly influential administrator officer for Vladimir Putin (Atwal, 2012). Besides, under Vasily Yakemenko as a supreme leader, *Commissar* positions were seated by Konstantin Goloskokov and Sergei Markov as two of the *Commissars* (Atwal, 2012). Konstantin Goloskokov and Sergei Markov pioneered the cyber-attack in Estonia at the same time when they were responsible as *Commissars* in Nashi Youth Group (Arnold, n.d.).

Second, Nashi Youth Group always receives a considerable amount of money from *Obshestvennaya Palata* (Public Chamber), a state financial institution in Russia (YAPICI, 2016). Also, Nashi Youth Group received direct funding of 6 million rubles in 2007 and more than 15 million rubles in 2008 only for Nashi Youth Group's *summer's forum* and some educational agenda (YAPICI, 2016). Moreover, Nashi Youth Group received 26 million rubles in 2007 – 2010 through the state contracts and the president's request (YAPICI, 2016). Therefore, the Nashi Youth Group is often called a Governmental Non-Governmental Organization (GO-NGO) (YAPICI, 2016).

Third, the Nashi Youth Group was established to execute Russia's interest in internal and external policies, which means that Russia has been involved with setting Nashi Youth Group and its goals and purposes (planning). Nashi Youth Group has plans and objectives to keep anti-orange sentiment between the Russian young people and prevent *coup d'etat* to the current Russian Government (YAPICI, 2016). They also have a political reason to facilitate the Russian government and Nashi Youth Group members in nepotism. Therefore the government can guarantee the loyalty of Nashi Youth Group for them (YAPICI, 2016). Besides, Nashi Youth Group has a foreign mission, which is to impress the international communities that many young people in Russia have loyalty to their Government (YAPICI, 2016). This foreign mission then leads to a xenophobic atmosphere and hatred towards anyone who opposes the Government (Arnold, n.d.). The xenophobic atmosphere was shown in 2007 at Annual Summer Camp in Seliger Lake when a picture of Urmas Paet (Estonia's Ministry of Foreign Affairs) was drawn with Adolf Hitler's mustache, and a

caption said that "Who is this if this is not an enemy?" (YAPICI, 2016). After at the same Annual Summer Camp, Nashi Youth Group members were petting a pig named Thomas Hendrik Ilves (Estonia's President) (YAPICI, 2016).

Fourth, the Nashi Youth Group is also under the supervision of Russia. Following the previous explanation about planning in Nashi Youth Group, the Nashi Youth Group's relationship with the Russian government gives each other reciprocal benefits. As for the Nashi Youth Group members, becoming a member of the group provides them higher opportunities to be a cadre party of United Russia *(Edinaiiya Rossiia)* and to be a staff in the ministries and other governmental institutions (YAPICI, 2016). Besides, the staff's recruitment is often held in Nashi Youth Group's Summer Camp or other programs (YAPICI, 2016). The Russian government also showed their support by visiting the Annual Summer Camp in Seliger Lake. In 2009, 2011, 2012, and 2014 Vladimir Putin, as the President of Russia, directly visited the Annual Summer Camp (Julie Hemment, 2012). Also, Gleb Pavlovsky (political consultant for Kremlin) and Vladislav Surkov (Deputy Chief of Staff) had been responsible as one of Nashi Youth Group's leaders (YAPICI, 2016).

Fifth, the Nashi Youth Group is also equipped with cyber-weapon. The cyber-weapon is not only used to attack Estonia in 2007, but it also used to attack one of Russia's Mass Media called *Kommersant,* in 2008 (Atwal, 2012). The attack started from Nashi Youth Group triggered with *Kommersant's* article said that Nashi Youth Group is a shame of Russia and does not represent their 'democratic' purposes (Atwal, 2012). The cyber-attack was shutting down *Kommersant's* website for five hours, and it was proved that Nashi Youth Group is the actor behind the cyber-attack from Kristina Potupchik's email (one of the secretaries for Nashi Youth Group) that commands the members to block and oppressed *Kommersant* (Atwal, 2012).

Following those proof of Overall Control, according to Yevgeny Volk, a Director of the Moscow Office of the Washington-Based Heritage Foundation, stated that the Russian government is likely to give silent approval to the perpetrator of the cyber-attack in Estonia (Arnold, n.d.), He also said that Nashi Youth Group is an organization formed and controlled by the Russian government and the xenophobic atmosphere in Nashi Youth Group is the fuel for their further action (Arnold, n.d.). Vladimir Pribylovsky, a founder and contributor of the *anti-compromat.ru,* also stated that Estonia's cyber-attack is highly possible to be funded by the Russian government or other parties that have interests (such as businessmen or politicians) with Vladimir Putin to launch the cyber-attack. Someone might have given Nashi Youth Group a command to launch the cyber-attack (Arnold, n.d.). Supported by one of NATO's member's statements, the cyber-attack was impossible to be done by a group of individuals. It needs a higher entity on its back as a guarantee (Arnold, n.d.).

Therefore, the classification of armed conflict in Estonia can be classified as IAC, which started from NIAC (internationalized armed conflict). The armed conflict's

escalation was supported by attribution with Overall Control and Tadic Case as a reference. The perpetrator of the cyber-attack in Estonia is the Nashi Youth Group. Still, the group was entirely under control by the Russian government, so that the armed conflict became IAC.

III. Current Regulation under International Humanitarian Law

The existing IHL ruled that there are some ways to begin applying IHL in IAC and NIAC, and as for the record, the beginning application of IHL in NIAC and IAC could be different. According to Common Article 2 of the Geneva Convention 1949, there are three ways to begin applying IHL, namely: declaration of war, hostilities between states, and occupation without armed conflict (International Committee of the Red Cross, 1949; Kolb, 2008). Also, Common Article 3 of Geneva Convention 1949 ruled that the IHL shall apply to NIAC as well as IAC with two thresholds that need to be fulfilled, which are the organized armed group and intensity of the conflict (Additional Protocols to the Geneva Conventions of August 12, 1949, 1977; International Committee of the Red Cross, 1949). Article 5 Geneva Convention III 1949 shall begin and apply when there is a person (as mentioned in Article 4) who falls into the enemy's power or commonly known as the prisoners of war (Geneva Convention III, 1949).

A. "Use of Force" under the UN Charter: *Jus ad Bellum v. Jus in Bello*

Before entering to explain further how the IHL begins and applies in Estonia's case, we need to comprehend the *jus ad Bellum* and *Jus in Bello* and why this matters for further discussion.

Article 2 (4) UN Charter stated that all UN members should refrain from the threat or use of force to other states that violate the state's jurisdiction (Charter of the United Nations and Statute of the International Court of Justice, 2014). This is also known as *Jus ad Bellum* that means 'the right to resort to force' or 'the right to wage war' (Kolb, 2008). The GA Resolution No. 3314 elaborates the definition of aggression to support the Article 2 (4) UN Charter (GA Resolution 3314, 1974). Article 1 of the GA Resolution No. 3314 said stated:

> *"Aggression is the use of armed force by a State against the sovereignty territorial integrity, or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this definition…"*

Referring to the definition above, aggression is an act of intervention, whether they are political or territorial, yet Article 3 of the GA resolution No. 3314 did mention the act of aggression, a cyber-attack is not one of them. However, the evolution of cyber-weapon could be used as a tool of war and political coercion, and yet this resolution is failed to adequately address this new weapon which could lead to keeping the attack occurred without clearly classifying it how far it could be a trigger of the beginning application of IHL or merely as an aggression act under this resolution (GA Resolution 3314, 1974).

In any legal system, including international law, this right is limited (Kolb, 2008). Article 51 UN Charter limits the use of force for self-defense purposes only or as a necessary action, taken by the Security Council, to maintain international peace and security (Kolb, 2008). However, the understanding of cyber-attack should be elaborated as well under Article 51 of the UN Charter, which means the cyber-attack should be equally applicable as self-defense. It is a natural right for a sovereign state to respond forcefully if it has been feeling attacked (Brierly, 2012). However, considering the phrase of aggression to the political independence of a state. The aggression using 'cyber' as its weapon should look carefully at what kind of impact that occurred or how the weapon is unleashed.

Rule 30 of Tallinn Manual 1.0 refers to the cyber-attack definition to an attack that give a physical impact on to person or object (CCD COE NATO, 2013). The definition from Rule 30 of Tallinn Manual 1.0 is different with spreading propaganda or psychological terror by using cyber-space as the media, the cyber-weapon in this issue is more relevant to the cyber-attack that gives physical impact to a person or object. Propaganda or psychological terror used with cyber as its media could be classified as a political intervention to a state, align with the mentioned phrase in GA Resolution No. 3314. However, discussing the aggression with cyber-attack could be tricky especially in differentiate between which one could trigger the beginning application of IHL. Rule 30 of Tallinn Manual 1.0 offered an answer and limitation of how far the application of cyber-weapon could be classified as an attack and trigger the beginning application of IHL, despite the reasons behind the attack, this explanation will be further discussed in another sub-topic specifically.

On the other side, *Jus in Bello* means the rules relating to the conduct of warfare (Kolb, 2008). *Jus in Bello* is the IHL itself. It does not consider why an armed conflict happened because once hostilities have begun, or a declaration of war has constituted a state of war, there is a need for some rules to regulate the relationships that arise as a result of the use of force or the state hostility (Kolb, 2008).

There is a little difference between *Jus ad Bellum* and *Jus in Bello,* and it might be tricky in Estonia's case since the attack was launched in cyber-space with a cyber-weapon. The cyber-attack in Estonia raised the question of whether it was enough to begin the application of IHL or not. Considering the hostility between Russia through Nashi Youth Group and Estonia, the thresholds seem enough to start the application of IHL. In cyber-attack, we need to look further at whether it only harms cyber-security (such as piracy, stealing, etc.) and could not trigger the beginning application of IHL or it was enough to be classified as an armed conflict. Julia Grignon, an expert in IHL, said that an attack launched by a party has to be caused by enmity, and it could not be caused by benevolence (Grignon, 2014). The 'enmity' here makes a big difference since one of the methods to begin applying IHL is hostility between states, yet an attack must follow the hostilities. Therefore, the motive of enmity is essential to determine the cyber-attack in Estonia so that it can be classified as an armed conflict or not.

Besides, following the Material Scope of IHL according to Robert Kolb and Richard Hyde, this article will only focus on the act of an attack that could trigger the beginning application of IHL (Kolb, 2008). Surely, the other scopes are equally important in determining a cyber-warfare under IHL, however, this article will solely focus on the material scope to see the threshold of a cyber-attack that could trigger the beginning application of IHL. Comparing Rule 30 of Tallinn Manual 1.0 with the existing regulations of IHL (Common Article 2 Geneva Convention 1949 and Article 49 (1) Additional Protocol I 1977), there are two points that differentiate Rule 30 of Tallinn Manual 1.0 from the existing regulations of IHL. The two points are the kinetical character of an attack and the physical impacts of an attack, which will be explained furtherly below.

B. Cyber-Attack in Geneva Convention 1949: Physical Impact v. Non-Physical Impact

Since the classification of armed conflict in Estonia had been determined as IAC, the Common Article 2 of the Geneva Convention 1949 shall apply to this case. Align with Robert Kolb and Richard Hyde's opinion on Scope of Material on IHL, Estonia's cyber-attack might begin with hostilities between states as the trigger. An attack followed the hostilities themselves. But the question is, does the Common Article 2 of Geneva Convention 1949 accommodate cyber-attack as the following act of hostilities? Paragraph 254 – 256 of Commentary 2016 on Common Article 2 of Geneva Convention 1949 (Commentary 2016) already stated cyber-attack in IHL. Yet, those paragraphs were not clear and firm enough to make thresholds about what kind of a cyber-attack could begin the application of IHL (Commentary 2016 on Geneva Convention I 1949, 2016). In Paragraph 254, the cyber-attack is accommodated under IHL to support a conventional war (Commentary 2016 on Geneva Convention I 1949, 2016), which means the war itself has already begun before the cyber-attack is launching. The polemic of cyber-attack will not be a problem in the Case of Stuxnet in Iran and Georgia v. Russia. The Stuxnet in Iran happened because the USA cooperated with Israel and attacked the Natanz Nuclear Plant in Iran with malware called Stuxnet (Kimberly Kagan, 2007). The virus was damaging the Natanz Nuclear Plant without even Iran realized it at first (Parker, n.d.). However, Iran, the USA, and Israel already waged war in a *proxy war* (Kimberly Kagan, 2007), which means that the conventional war had already begun long before the Stuxnet was launched at Natanz Nuclear Plant.

The Stuxnet in Iran, Georgia v. Russia, both of them had been involved in the separatist movement in South Ossetia, one of Georgia's provinces, since 1991 (Tikk, 2010). Even though a truce and consolidation for peace, the tense was never gone in South Ossetia (Tikk, 2010). In Georgia, the cyber-attack first happened on July 19, 2008, by using DDoS (the same method as the cyber-attack in Estonia) (Tikk, 2010). The cyber-attack was continued until August 7, 2008, when Georgia attacked the separatist movement in South Ossetia supported by Russia and countered by Russia on the next day (Tikk, 2010). Also, Mikheil Saakashvili, Georgia's President, declared that the state is at war and Russia has done aggression to Georgia (Tikk, 2010). Considering Paragraph 254 of the Commentary 2016, the cyber-attack, in this

case, will not be a problem for the case of Georgia v. Russia since the tension has not fully recovered since 1991. There was also a conventional attack from both parties and followed by a declaration of war by the President of Georgia.

Nevertheless, this paragraph could not be applied to the Case of Estonia since the attack was entirely made in cyberspace without any kinetical or conventional attack that can begin the application of IHL. Paragraph 255 of Commentary 2016 tried to answer this problem by stating that a cyber-attack might trigger the beginning application of IHL if it has a physical impact (Commentary 2016 on Geneva Convention I 1949, 2016). The physical consequences mean that the cyber-attack could injure or kill a person and damage or destroy an object (Commentary 2016 on Geneva Convention I 1949, 2016). However, the next paragraph (Paragraph 256) stated that a cyber-attack could also have a non-physical impact that could not be seen or felt. This paragraph had not firmly concluded that what kind of impact that cyber-attack could begin the application of IHL (Commentary 2016 on Geneva Convention I 1949, 2016).

However, considering the physical impact in the case of Estonia, such as disturbance and damage to public transportation and water supply at Tallinn, the cyber-attack in Estonia is under the para. 255 of Commentary 2016 on Common Article 2 Geneva Convention 1949. Regardless of the indecision of this article, this article could be a legal basis for triggering the beginning application of IHL.

C. Cyber Attack in Additional Protocol I 1977: Kinetic Attack v. Non-Kinetic Attack

Following Common Article 2 of Geneva Convention 1949, we had to look at the definition of attack under Article 49 (1) Additional Protocol I 1977. One of the debatable topics in cyber-attack under IHL is whether an attack had to be kinetic or not to legalize the beginning application of IHL. Article 49 (1) Additional Protocol I 1977 didn't require an attack to be a kinetical attack to begin the application of IHL, considering a cyber-attack is a non-kinetic attack. This article seems promising to accommodate cyber-attack under IHL. According to W.J. Hurley, a kinetical character means using a physical power and system to support that physical power (such as using a military vehicle or sensor to detect and help shoot a target, etc.) (Hurley, 2009). In the polemic of cyber-attack, whether an attack should be kinetical or not is essential. In practice, the kinetical attack is attached to a conventional attack, and it could always be sensed by humans' sensory perceptive (it can be seen how the weapon works or how the vehicle moves). Therefore, it is easy to determine the beginning application of IHL.

Unfortunately, this article is inconsistent in defining whether an attack should be kinetic or not. Even though the article did not state about a requirement to be kinetic, Paragraph 1880 of the Commentary Article 49 (1) Additional Protocol I 1977 (Commentary of AP I 1977) stated that the attack should be applied equally in terms of counterattacks as a defense (Additional Protocol I to the Geneva Conventions of

August 12, 1949, 1977). By this counterattack means, the commentary firmly said and focused on combat action, which referred to non-kinetic attack (Additional Protocol I to the Geneva Conventions of August 12, 1949, 1977). It means that armed forces should do a counterattack in combat action with a real physical weapon. Meanwhile, a cyber-attack can be done by anyone outside the armed forces. Therefore, this article could not give a firm answer to cyber-attack thresholds in terms of kinetic or not.

IV. Cyber-Attack in Tallinn Manual 1.0

Before getting into a further discussion of the cyber-attack in Tallinn Manual 1.0, this discussion will not be making Rule 30 of Tallinn Manual 1.0 as a legal basis for triggering the beginning application of IHL in the case of Estonia. Yet, this discussion will compare the Common Article 2 of Geneva Convention 1949 and Additional Protocol I 1977 with Rule 30 of Tallinn Manual 1.0.

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*" (CCD COE NATO, 2013). Referring to that rule, 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. However, Tallinn Manual 1.0 does not provide further explanation as to what extent this attack can trigger the applicability of the IHL. Therefore, it is necessary to have a close examination of each of those elements mentioned above.

First, 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 "*connected with electronic communication networks, especially the internet*" (Oxford English Dictionary, 2020a). Meanwhile, the word 'operation' means "*an act performed by a machine, especially a computer*" (Oxford English Dictionary, 2020b). In the military topic, "*operation is a military activity*" (Oxford English Dictionary, 2020b). 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 (CCD COE NATO, 2013).

Second, the element of 'to offense or defense' is also 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, commentary of Rule 30 Tallinn Manual 1.0 states that an attack should not only limited to a kinetic attack but also has to be applied equally to a non-kinetic attack (CCD COE NATO, 2013), which 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' (CCD COE NATO, 2013). This is in line with Julia Grignon's opinion that an

attack must be launched based on enmity (Grignon, 2014). It is reflected in Estonia's case since strong evidence that the hostilities exist in Nashi Youth Group is reflected by their xenophobic atmosphere. Therefore, the element of 'enmity' is met in this case and could legitimize the cyber-attack

Third, the element of 'expecting to cause …' also distinct the Rule of 30 Tallinn Manual 1.0 with Common Article 2 Geneva Convention 1949, which could not determine whether a physical on the non-physical impact that could trigger the beginning application of IHL. According to paragraph 5 of this rule's commentary, the effects should be an expected physical impact (CCD COE NATO, 2013). By this expected means, a cyber-attack that launched will cause harm to a person or an object physically, even though the impact was not directly shown or felt by the target (CCD COE NATO, 2013). 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 in Article 49 (1) Additional Protocol I 1977 use an analogy of mines that buried down into the ground is guaranteed to give a physical impact both for a person or an object, even though the impact has not been made, the attack is still considered has launched (Additional Protocol I to the Geneva Conventions of August 12, 1949, 1977). 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 (Hermawan, S, 2020) yet those three could cause harm to a person, both injured or dead, and still regulated as an attack under the existing IHL (CCD COE NATO, 2013). As well as those three weapons, the cyber-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 of 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 (Zetter, 2014). Indeed, the cyber-attack gave massive physical damage to Natanz Nuclear Plant slowly that Iran didn't know for a year (Zetter, 2014).

Moreover, the commentary Rule 30 Tallinn Manual 1.0 is admitting and affirming 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*"(HPCR, 2009). According to that definition and general feeling concept in Tallinn Manual 1.0, we can see that both focus on the purpose of the attack that is giving physical impacts. It means Rule 30 Tallinn Manual 1.0 also has answered the legality of cyber as a weapon to attack either offense or defense. Comparing the definition of cyber-attack in Rule 30 of Tallinn Manual 1.0 with some definitions from other states, this definition is still more comprehensive and acceptable than from other states. First, U.S. National Research Council's Committee on Offensive Information Warfare (NRC Committee) defines cyber-attacks as referring to, "deliberate actions to alter, disrupt, deceive, degrade, or destroy computer systems or networks or the information and/or programs resident in or transiting these systems or networks" (Peagler, 2014). Second, the Shanghai Cooperation Organization focusing the definition of cyber-attack to information warfare, as an act by a state to disrupt the social system,

economy, and politics of another state (Kilovaty, 2014). The definition from the US and China are not comprehensive enough comparing with the definition of cyber-attack by Rule 30 of Tallinn Manual 1.0.

The US' definition is not stating about the physical impacts that might and surely be occurred to a person or object, which important as a threshold of a cyber-attack in triggering the beginning application of IHL. As well as the US' definition, China's definition also does not include the physical impact and it is focusing on information warfare. Equalizing the definition of cyber-attack with information warfare could be tricky to determine the beginning application of IHL. China's definition is related to the definition of aggression under the GA Resolution No. 3314 and could be started as political interference with no actual physical harm to a person or an object. It means, the cyber-attack with only propaganda and psychological terror with no physical harms could not trigger the beginning application of IHL, and the position of the cyber-attack is only classified as mere aggression (Jus ad Bellum) without complying the Jus in Bello. Overall, those two definitions are not enough to answer this issue and are hardly accepted by other states since the definitions surely adjusted with their political interests.

As well as the definition from US and China, the previous explanation of how Rule 30 Tallinn Manual 1.0 comprehensively answer this issue has also answered the missing explanation of cyber-attack in the definition of aggression under GA Resolution No. 3314. After determining the definition of cyber-attack, the further definition that needs to be agreed with all states is the definition of cyber-warfare. As a reference, the definition of cyber warfare has been expanded to include government-sponsored espionage, potential terrorist attacks in cyberspace, large-scale criminal fraud, and even hacker kids attacking government networks and critical infrastructure (Peagler, 2014). Indeed, this definition is required more discussion and agreement from many states, which will be a further discussion that could explore by other scholars or practitioners. Regardless of the definition of cyber-warfare, the cyber-attack definition under Rule 30 of Tallinn Manual 1.0 is comprehensive enough in solving the cyber-attack issue in terms of triggering the beginning application of IHL.

Therefore, Estonia's cyber-attack also aligned with Rule 30 of Tallinn Manual 1.0 since the act of hostilities between Russia and Estonia and the physical impacts such as Tallin's water supply and transportation railway had reflected in Rule 30 of Tallinn Manual 1.0. Although the Tallinn Manual 1.0 is not one of the sources of international law and could not legally binding, the cyber-attack in Estonia had drawn attention from the international community, such as from NATO and *European Network and Information Security Agency* (ENISA), which had done simulation, system repairing, reorganization, and many other things, are the proof that this case brings a new urgency to international law (Herzog, 2011). It means that this case brings new urgency to global communities to legitimize the Rule of 30 Tallinn Manual about cyber-attack as support binding regulation for Common Article 2 of the Geneva Convention 1949.

Although the establishment of a new norm from the Rule 30 Tallinn Manual 1.0 to become a customary international law is hard, it is still possible to become customary international law. The reason is that customary international law required a general

practice and a consensus of the newly emerging practice from the states, yet the existing international law tend to focus on cyber issues related with trade law, trademark law, or any issues besides the IHL issue (Arend, 2003). However, despite the Rule 30 of Tallinn Manual 1.0 is not a source of international law and could not be legally binding, those findings lead to another question about the status of Tallinn Manual 1.0, especially Rule 30 of Tallinn Manual 1.0. In addition, following NATO and ENISA, some states had also established a practice whether by building a cyber armed-forces or established a regulation related to the cyber-warfare as a preparation and prevention act. This could be a sign that general practice has to emerge initiated from Rule 30 of Tallinn Manual 1.0, which could lead to emerging of a new customary international law in the future.

V. Conclusion

Estonia's cyber-attack could be classified as an International Armed Conflict (IAC), which first started as Non-International Armed Conflict (NIAC) by proving attribution from Russia to Nashi Youth Group following the Overall Control in Tadic Case. Since the armed conflict is IAC, the beginning application of IHL, in this case, could begin with hostilities between states followed by cyber-attack under Common Article 2 Geneva Convention 1949 and supported by Rule 30 of Tallinn Manual 1.0 as a non-binding regulation. These findings could give us a new perspective and answer of how a cyber-attack could trigger the beginning application of IHL as it has happened to Estonia.

This topic will keep growing furtherly in more discussions to come considering the cyber-attack regulations under IHL are not fully established, but the topic in this article about the beginning application of IHL caused by a cyber-attack will give a better and firmer understanding of this issue. This article also discussed how a cyber-attack is different from information warfare, which makes the definition of aggression under GA Resolution No. 3314 is not capable of answering this issue. The distinction between information warfare and cyber-attack is related to the physical impact of a cyber-attack, which a threshold of a cyber-attack under Tallinn Manual 1.0. It means the Rule 30 of Tallinn Manual 1.0 also answered the threshold of *Jus ad Bellum* and *Jus in Bello* in terms of cyber-attack.

The investigation of the cyber topic under IHL will keep expanding to more advanced matters, the beginning application of IHL was only the start of discussion to trigger many questions to come, such as the fixed and acceptable definition of cyber-warfare. The authors hope to make a contribution to the development issues of the cyber-attack under IHL, specifically about how a cyber-attack could trigger the beginning application of IHL. Although this article needs some improvements regarding the limitation of this issue only focused from Material Scope of IHL, according to Robert Kolb and Richard Hyde, we hoped to see a more intriguing discussion to expand our knowledge of this matter and more contribution for answering the cyber-attack issues under the IHL. In addition, the Rule 30 of Tallinn Manual 1.0 is not legally binding because it is not one source of international law, however it is possible for the Rule 30 Tallinn Manual 1.0 to be a new norm and becoming customary international law in the future.

References:

Books:

Amazon Web Services. (2019). *AWS Best Practices for DDoS Resiliency*.

Arnold, C. (n.d.). *Russian's Group Claims Reopen Debate on Estonian Cyber Attacks*. Retrieved August 29, 2020, from https://www.rferl.org/a/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html

Atwal, M. and E. B. (2012). The Youth Movement Nashi: Contentious Politics, Civil Society, and Party Politics. *East European Politics*, *28*(3).

Brierly, J. L. (2012). Brierly's Law of Nations. *Brierly's Law of Nations*. https://doi.org/10.1093/law/9780199657933.001.0001

Cassese, A. (2007). The Nicaragua and Tadić Tests revisited in light of the ICJ judgment on genocide in Bosnia. *European Journal of International Law*, *18*(4), 649–668. https://doi.org/10.1093/ejil/chm034

CCD COE NATO. (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual 1.0). In M. N. Schmitt (Ed.), *NATO* (Vol. 82, Issue 12). https://doi.org/10.5325/j.ctv14gpdw3.13

HPCR. (2009). Manual on International Law Applicable to Air and Missile Warfare. In *Group*.

Kolb, R. and R. H. (2008). *An Introduction to the International Law of Armed Conflicts*. Hart Publishing.

Sassoli, M. (n.d.). How Does Law Protect in War? In *ICRC Online Casebook*. https://casebook.icrc.org/glossary/internationalized-internal-armed-conflict.

Tikk, E. (2010). *International Cyber Incidents Legal Considerations*. CCD COE.

Zetter, K. (2014). *Countdown to Zero Day Stuxnet and the Lunch of the World's First Digital Weapons*. Crown Publishers.

Legal Documents:

Additional Protocols to the Geneva Conventions of August 12 1949, 30 (1977). https://www.icrc.org/eng/assets/files/other/icrc_002_0321.pdf

Charter of the United Nations and statute of the International Court of Justice, 3 (2014). https://doi.org/10.18356/c89fd759-en

Commentary 2016 on Geneva Convention I 1949, (2016).

Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, Prosecutor V.Dusko Tadic A/K/A "Dule," (1995).

GA resolution 3314, Pub. L. No. 3314 (1974). https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/3314(XXIX)

Geneva Convention III, (1949).

ICRC. (2008). *How is Term "Armed Conflict" Defined in International Humanitarian Law* (Opinion Paper).

International Committee of the Red Cross. (1949). *The Geneva Conventions of August 12 1949. August*, 224.

Opinion and Judgement on Prosecutor v. Dusko Tadic A/K/A "Dule," (1997).

Walter, C., Vöneky, S., Röben, V., & Schorkopf, F. (2004). *Draft Articles on Responsibility of States for Internationally Wrongful Acts (2001). II*, 1465–1482. https://doi.org/10.1007/978-3-642-18896-1_61

Articles:

Arend, A. C. (2003). International law and the preemptive use of military force. *Washington Quarterly*, *26*(2), 89–103. https://doi.org/10.1162/01636600360569711

Atwal, M. and E. B. (2012). The Youth Movement Nashi: Contentious Politics, Civil Society, and Party Politics. *East European Politics*, *28*(3).

Cassese, A. (2007). The Nicaragua and Tadić Tests revisited in light of the ICJ judgment on genocide in Bosnia. *European Journal of International Law*, *18*(4), 649–668. https://doi.org/10.1093/ejil/chm034

Grignon, J. (2014). The beginning of application of international humanitarian law: A discussion of a few challenges. *International Review of the Red Cross*, *96*(893), 139–162. https://doi.org/10.1017/S1816383115000326

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security*, *4*(2), 49–60. https://doi.org/10.5038/1944-0472.4.2.3

Hurley, W. J. (2009). Non-Kinetic Capabilities for Irregular Warfare: Four Case Studies. In *Institute for Defense Analysis Paper*.

Julie Hemment. (2012). Nashi, Youth Voluntarism, and Potemkin NGOs: Making Sense of Civil Society in Post-Soviet Russia. *Slavic Review*, *71*(2), 234. https://doi.org/10.5612/slavicreview.71.2.0234

Kilovaty, I. (2014). Cyber Warfare and the Jus Ad Bellum Challenges: Evaluation in the Light of the Tallinn Manual on the International Law Applicable to Cyber Warfare. *American University National Security Law Brief*, *5*(1), 4.

Peagler, J. (2014). The Stuxnet Attack: A New Form of Warfare and the (In)applicability of Current International Law. *Arizona Journal of International and Comparative Law*, *31*(2), 399–434.

Hidayat, S. N., Karjoko, L., & Hermawan, S. (2020). Discourse on Legal Expression in Arrangements of Corruption Eradication in Indonesia. *JILS (Journal of Indonesian Legal Studies)*, *5*(2).

Marttinen, K. (2016). *State Responsibility for Genocide – The International Court of Justice's Judgment in the Genocide Case and its Aftermath*. http://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=8897226&fileOId=8900463

NATO. (n.d.). *2007 Cyber Attacks on Estonia*. Thematic Area: Cyber Operations. https://webcache.googleusercontent.com/search?q=cache:O8F8g08TxSQJ:https://www.stratcomcoe.org/download/file/fid/80772+&cd=8&hl=en&ct=clnk&gl=id

Ottis, R. (2008). Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective. *7th European Conference on Information Warfare and Security 2008, ECIW 2008*, *April*, 163–168.

YAPICI, M. İ. (2016). What Role Did Nashi Play in Russian Internal Politics and Foreign Policy A Formulator or an Implementer? *Review of International Law and Politics*, *12*(2), 1–1. https://doi.org/10.19096/rilp.2016216812

Schmidt, A. (2013). The Estonian Cyber Attacks. In J. Healey (Ed.), *The Fierce Domain Conflicts in Cyberspace 1986 - 2012*. Atlantic Council.

Website:

Arnold, C. (n.d.). *Russian's Group Claims Reopen Debate on Estonian Cyber Attacks*. Retrieved August 29, 2020, from https://www.rferl.org/a/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html

Kimberly kagan. (2007). Iran's Proxy War Against U.S. and the Iraqi Government. *Institute for the Study of War*. http://www.understandingwar.org/report/irans-proxy-war-against-united-states-and-iraq

Parker, D. (n.d.). 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/iran-timeline.html#/#time5_211