THE LIMITATION OF CYBER WARFARE UNDER HUMANITARIAN LAW
(Pembatasan Perang Siber dalam Hukum Humaniter)

Amalia Zuhra
Laila Almira
Faculty of Law, Universitas Trisakti
laila25almira@gmail.com

Abstract
States and non-State armed groups are increasingly employing cyber capabilities in their military operations in the digitalization environment today. There is a controversy about how current international legal frameworks, especially International Humanitarian Law (IHL), applies to such conduct in cyberspace, most notably in the context of armed conflict. Because one of the fundamental aims of the IHL is to protect civilians from the impact of armed conflict, it is critical to explore the norms of IHL that regulate such operations. This article will be likely to discuss about cyber warfare in the term of armed conflict. Lastly, the article will be reviewing the rules and principle that applies during the cyber warfare.

Keywords: Cyber warfare; cyber-attack; distinction principle; proportionality principle; precautionary measure.

Introduction
The developments of new technologies have changed our social, economic, business and philosophy. Presently, a State cannot function optimally without utilizing the technology since it is dependent on the computer, computer technology information, information technology, internet, etc. (Islam, 2017, p. 102).
In this twenty-first century, the information ethnology often uses in every stage and step of life to conduct business, i.e., payroll and accounting, recording inventory and sales, research, transportation, health care, financial services, manufacturing products in factories, managing military forces, for distribution networks for food, water and energy. However, it also opens the possibility of cyber-attack and damage to the states and civilians (Islam, 2017, p. 102).

It must be noted that there is plenty of state conflicts where cyber was utilized as a weapon in this century. Some cases that highlight the existence of cyber operations begin on September 11, where the transnational terrorist attacked the pentagon, followed by the cyber operations against Estonia in 2007 and against Georgia in 2008, in 2010 Stuxnet worm attack on Iran nuclear facilities. (Schmitt, 2017, p. 376) The first global cyber-attack happened in 2017 in developing a “ransomware” attack named WannaCry, where hundreds of thousands of computer networks were infected in 150 countries, resulting in losses of up to $4 billion. This attack also affected thousands of civilian infrastructures (i.e. hospitals, transport services, energy services, etc.) (Hollis, 2018, p. 1).

Throughout history, the nature of conflict has evolved. In a world that has entered the digital era in this century, conventional wars are unlikely to be frequent occurrence. However, this does not mean that it can be concluded that the world is already safe. The era of digitalization has led humans using internet technology to accept the fact that armed conflicts can also occur in cyberspace. Today, cyber warfare has become the newest battleground. The term cyber warfare defines “to warfare conducted in cyberspace through cyber means and methods”.

While warfare is commonly referred to as “conduct of military hostilities during armed conflict”, cyberspace is “a globally interconnected network of digital information and communication infrastructures, including internet, telecommunications networks, computer systems and the information resident therein”. Cyber warfare is conducted in cyberspace, may produce effects outside the cyber domain, and in some situations, this could be the outcome desired by the attacker (Melzer, 2011, p. 4).

The term “cyber warfare” covers both cyber weapons and cyber weapon systems. The term of cyber-attack is defined as “Cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to person or damage or destruction to object” (Schmitt, 2008, p. 152).

International Humanitarian Law (IHL) regulates all means and methods of warfare, including the use of all weapons manifested in Art. 36 of Additional Protocol I, which quoted:

“In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party” (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 36).

According to the Commentary of Additional Protocol I, this article is the only one which establish a link between its provision, especially the basic rules on the means and methods of warfare, and the introduction of a new weapon by States. The most important thing of this article lays its mandate to the State Party to determine the possibly unlawful nature of a new weapon, both with regard to the provision of the Protocol, and to any other rule of international law. The first and foremost obligation of State Parties was excellently formulated in order to underline the important reason of using a new weapon: “that the determination of the legality of a new weapon is not intended to create a subjective standard, but such determination will ensure that means and methods of warfare will not be adopted without the issue of legality being explored with care, that it requires States to analyze whether the employment of a new
weapon is for its normal or expected use would be prohibited under some or all circumstances. It states also that a State is not required to foresee or analyze all possible misuse of a weapon, for almost any weapon can be misused in ways that would be prohibited”.

IHL did not prohibit armed conflict. IHL is a set of rules aimed at limiting the effects of armed conflicts for humanitarian reasons. Based on the explanation mentioned above, this paper provides an insight into some of the ways in which key core concepts and legal parameters of IHL apply in the cyber warfare and how IHL limit the cyber warfare. The topic is limited to *jus in bello*.

**Cyber warfare as armed conflict**

IHL distinguishes two types of armed conflict, namely international armed conflict and non-international armed conflict. The question is how to determine armed conflict in the context of cyber warfare. The following paragraphs below will explain further, how a cyber-attack can be qualified as a cyber war, both in international armed conflicts or non-international armed conflicts.

**International Armed Conflict (IAC)**

For IAC to exist Article 2 common to all four Geneva Convention which stated that:

"In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance” (Geneva Convention Relative to the Protection of Civilian Persons, Art. 2).

From the provision, we should note that the IAC existed “whenever there is a resort to armed force between states”, (International Criminal Tribunal for the Former Yugoslavia 1993-1998, 1999, p. 70) in Gombo, “IAC exists in case of armed hostilities between States through their respective armed forces or other actors acting on behalf of the State”. (International Criminal Court, 2009, p. Para. 223) There is no necessity that IAC must reach a specified level of intensity before an armed conflict exists. Moreover, Art.2 did not contain a minimum threshold for the intensity or duration of hostilities to establish the IAC (Pictet, 1958, p. 20).

The most exciting part of this section is the fact that in cyber operations, however, there is no kinetic force. The fundamental point of debate is whether the use of kinetic force is required for “armed conflict” to exist under IHL.

To answer this, some scholars conclude that if a State is responsible for a cyber-attack, the cyber-attack has the same effects as a kinetic force (Chang, 2017, p. 31). Therefore, it will lead us to Responsibility of States for Internationally Wrongful Act that explains the line of attribution of conduct to a state which includes if that act “committed by the organs of a State, exercising elements of government authority, organs placed at the disposal of a State by another State, excess of authority or contravention of instructions, directed or controlled by a State, carried out in the absence or default of the official authorities, the conduct of an insurrectional or other movements, acknowledge and adopted by State” (Chang, 2017). Thus, it can be said that the IAC exist.
Non-International Armed Conflict (NIAC)

To establish whether cyber activities alone could lead to the creation of NIAC, it must be determined whether, and if so, under what circumstances, the required “threshold of violence” and “degree of organization” with regard to the armed group involved is met (International Criminal Court, 2009, para. 231).

In Gombo, (International Criminal Court, 2009, para. 231) the intensity level “should reach a higher threshold beyond mere internal disturbances and tensions, such as riots, isolated and sporadic acts of violence, and other acts of a similar nature” (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 1 (2)).

It is not easy to establish the level of intensity in the context of cyber operations. It appears that no cyber-attack has reached the required level of intensity. Even the Stuxnet operation, the most famous cyber operation that caused physical destruction in the “real world” and internet riots by the Russian minority in Estonia, did not approach the threshold of violence required for NIAC. (Brown & Poellet, 2012, p. 132) Moreover, singular and merely sporadic cyber incidents, even if they causes physical damage or injury does not constitute as NIAC.

Tallinn Manual noted that there are other criteria to assert to establish the threshold such, as:

“the gravity of attacks and their recurrence; the temporal and territorial expansion of violence and the collective character of hostilities; whether various parties are able to operate from a territory under their control; an increase in the number of government forces; the mobilisation of volunteers and the distribution and type of weapons among both parties to the conflict; the fact that the conflict has led to a large displacement of people; and whether the conflict is the subject of any relevant scrutiny or action by the Security Council”.

Moreover, in this case, a computer network attack (CNA) or computer network exploitation (CNE) would fall in the sense of “attack” under Art. 49 and if carried out in the midst of already-existing armed conflict (Geiss, 2013, p. 634).

Another point that needs to establish is “some degree of organization”. In that regard, Limaj has focused on the following indicia of organizational capacity, which are “a demonstrable hierarchy, the existence of a uniform, the ability to procure, transport, and distribute arms, and the capacity to coordinate its actions” (International Criminal Tribunal for the Former Yugoslavia 1993-1998, 2005, para. 90-123.).

In this regard, the expert agrees that “virtual groups”, i.e., groups that consist of people spread across multiple areas and solely on the internet, cannot be regarded as organized armed groups due to the impossibility to determine the natural person and the membership of the group. Geiss, Op. Cit., 636.

If these requirements are present meaning the NIAC exists.

Cyber-attack amounting to an attack under IHL

Cyber-attack refers to CNA or CNE (Lehm, 2013, p. 6.). The CNA encompasses all cyber operations intended “to disturb, deny, degrade, or destroy information resident in computers and computer networks, or computers and networks themselves”. While CNE refers to “enabling operations and intelligence collection to gather data from target or adversary automated information systems or networks” (Melzer, 2011, p. 5).

To establish the applicability of IHL to the cyber-attack, it must be noted that the expert in the drafting of the Tallinn Manual includes the situation of armed conflict. Therefore, the
cyber-attack only occurs if there is a nexus between the cyber activity and the armed conflict to that activity (Schmitt, 2008, p. 376). Furthermore, the experts also make a distinction between international armed conflict cyber-attacks and non-international armed conflict cyber-attacks in Rules 82 and 83 (Schmitt, 2008, pp. 379–385).

The term of “attack” defined in Art.49 (1) Additional Protocol I as: “act of violence against the adversary, whether in offence or defence”. (Protocols Additional to the Geneva Conventions of 12 August 1949, p. Art. 49 (1) However, cyber operations are a new development of technology, it raising the question does such definition extent to cyber operation.

The fact that cyber operations cannot exclude IHL from applying to cyber operations. This can be concluded from the Case of Nuclear Weapon, where it stated clearly that IHL applies “to all forms of warfare and to all kinds of weapons”, including “those of the future” (International Court of Justice, 1996, p. 86).

Today, it appears that acts of violence does not always necessitate the use of kinetic violence. However, it suffices if the resultant effects are comparable to the traditionally associated with kinetic violence, namely the death or injury of people or the physical damage of items. With this, we can conclude that cyber operations result in a loss of functionality without causing physical damage (Melzer, 2011, p. 5). In addition, cyber operation that is directed to the civilian network (electricity, banking, or communications) can be said as an integral part of an “act of violence” within the meaning of Art. 49(1) of Additional Protocol (Schmitt, 2012, pp. 289–290).

**Principle and Rules apply for cyber-attack**

The concepts of distinction, proportionality, and precaution, as well as the interpretation of those norms in the cyber space, are governed by IHL. In light of all of these regulations, the cyber realm raises a lot of unanswered questions (Droege, 2012, p. 534).

The law of targeting is based on the concept of limiting the amount of violence that parties to a conflict may lawfully utilize during an armed conflict in order to provide civilians with the best possible protection.

**The principle of distinction**

This principle has been manifested in the Art.48 of Additional Protocol I and Rule 93 Tallinn Manual 2.0. (Schmitt, 2017, p. 420). It must be highlight that this poses a serious challenge to establish this one of two cardinal principles of IHL, to make the difference between military and civilian objects in jeopardy (Droege, 2012, p. 539).

The civilian objects are all objects which not military objectives. Meanwhile, the military objectives shall be assessed from the nature, location, purpose, or use to make an effective contribution to military action. In addition, the total or partial destruction, capture or neutralization which in the circumstances ruling at the time offers a definite military advantage. According to the Commentary of Additional Protocol I, these two requirements should be both present in order to determine a military objective in the perspective of the Additional Protocol I. Although the expression of “a definite military advantage” used in Art. 52 is very similar to other term of “concrete and direct military advantage anticipated” used in other articles of Additional Protocol I, but according the Commentary, the Art. 52 provides that there must be a definite military advantage for every military objective that is attacked (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 52 (1) (2)).
The assessment of effective contribution, such object must use for combat that military in nature. A war-fighting object in the cyber environment would be a weapon's computer guidance system or classified network on which military operations are planned and executed (Pascucci, 2017, p. 433).

The 'nature' refers to an inherent characteristic or attribute which contributes to military action. 'Location' defines as geography that special importance to military action (Pascucci, 2017, p. 435). If the state has dual-use objects in cyberspace, such as part of the civilian infrastructure that supplies the military for their operations, such as power plants or electrical grids. The principles of precautions and proportionality must be followed (Droege, 2012, pp. 562, 564) ‘Purpose’ highlighted by the recent use (e.g., command and control, propaganda, inciting violence) of social media (e.g., Facebook, Twitter, etc.) by the parties to the conflict (Pascucci, 2017, p. 437).

From this standpoint, during cyber warfare operations, the commander must plan and coordinate all measures possible to ensure that targeted objectives are not civilians or civilian objects. The fact that the military and civilian computers or computers systems are not entirely one and the same (Droege, 2012, p. 539).

Moreover, as a protective device, there are visible symbols of the special protection under IHL for specific categories of people, units, and transports (particularly medical personnel, facilities and means of transport) (ICRC), 2011, p. 25).

The question arises about distinctive emblems in the context of cyber warfare. The idea of creating a new signal, digital marking, or other means of cyberspace identification, namely digital emblem, has emerged. It can be distinctive emblems or distinctive signals such “as light, radio and electronic signal”. However, it is still in the discussion and need more development and tested (Rodenhauser et al., 2021).

**The principle of proportionality**

The principle of proportionality underpins the restriction on indiscriminate attacks and is intended to counteract the principle of distinctions otherwise "inadequate“ protection of the civilian population, civilians, and civilian property (Pascucci, 2017, p. 445).

This rule is based on Arts. 51 (5) (b) and 57 (2) (iii) of Additional Protocol I, Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 52 (5) (b)., and rule 113 of Tallinn Manual 2.0. (Schmitt, 2017, p. 471).

Proportionality determined the degree and kind of force used to archive a military objective by comparing the predicted military advantage gained to the expected incidental damage inflicted on civilians and civilian property (Pascucci, 2017, p. 445).

In the context of cyber operation, if such attack is reasonably expected to cause a temporary disruption to a public-facing website but results in unanticipated destruction of a server hosting medical records, culminating in patient deaths, the proportionality principle is met as long as the expected temporary disruption to the public-facing website is not excessive in nature (Pascucci, 2017, p. 446). The reason behind this is because cyber-attacks on military objectives sometimes launch via civilian communication cables, satellites, or other infrastructure. Furthermore, explain that cyber-attack can cause collateral damage (Schmitt, 2008, p. 471).

In the case of the dual-use cyber infrastructure that qualifies as a military objective but at the same time, it performs essential civilian functions. For illustration when 10% of the capacity of a central server is used for military reasons, while 90% is used for civilian operations. As a result, the server qualifies as a legal military objective. This is because any
military application, no matter how minor, qualifies an entire object as a lawful military objective (Geiß & Lahmann, 2012, p. 397).

However, it is prohibited if the collateral damage is excessive to the concrete and direct military advantage. This statement needs more assessment of the reasonableness of the determination at the time (Schmitt, 2017, p. 474). Moreover, as noted in Galić to determine the attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, using reasonable use of the information available to him or her, could have expected excessive civilian causalities as a result of the attack (International Criminal Tribunal for the Former Yugoslavia 1993-1998, para. 58).

**The principle of precaution**

This principle has two aspects which include precautions in attack and precaution against the effect of attacks. (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 48, 49.).

Under this principle, IHL mandates that all reasonable efforts be made to verify that targets are military objectives, (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (a) (i)) as well that all feasible precautions in the selection of means and methods of warfare with the goal of avoiding or, at the very least, minimizing incidental civilian causalities and damage to civilian casualties and damage to civilian objects (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (a) (ii)). It also mandates that if it becomes clear that an attack would inflict considerable "collateral damage", the parties to the dispute must cancel or suspend the attack (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (2) (b)).

Many States has defined the word "feasible": “as being limited to those precautions which are practicable or practically possible, taking into account all circumstances ruling at the time” (Henckaerts & Doswald-Beck, 2005, p. 54.).

However, in the cyber, “feasible precautions” must be related to technology. In this case, the commander should be making sufficient maps of the networks adequately to assess the attack's consequences, particularly on the civilian and civilian objects (Jensen, 2013, p. 202).

In addition, when deciding between various military objectives with a similar military advantage, the attacker must take ‘constant care’ and ‘reasonable precautions’ to spare the civilian population and civilian objects (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 57 (1)).

In the cyber context, the ‘constant care’ means the entire person involved must be continuously sensitive to the effect of their activities at all times, not merely during preparation (Schmitt, 2017, p. 474).

The precautions against the effect of attacks require parties to the conflict “to the maximum extent feasible.....to remove the civilian population, individual civilians and civilian objects under their control” (Protocols Additional to the Geneva Conventions of 12 August 1949, Art. 58).

However, in the context of cyber Tallinn Manual states, certain actions that need to be taken include:

*segregating military from civilian cyber infrastructure; segregating computer systems on which critical civilian infrastructure depends from the Internet; backing up important civilian data elsewhere; making advance arrangements to ensure the timely repair of
important computer systems against foreseeable kinds of cyber attack; digitally recording important cultural or spiritual objects to facilitate reconstruction in the event of their destruction during armed conflict; and using antivirus measures to protect civilian systems that might suffer damage or destruction during an attack on military cyber infrastructure” (Schmitt, Op. Cit., 488).

Unlike other principles that mention about the condition of dual-use, this principle strictly prohibited the dual-use and stated that it should keep distinct.

Conclusion

Cyber warfare requires new means and methods of warfare, some of the impact of which have yet to be verified or understood. The military use of technology information looks to offer severe problems to the application of IHL. Cyber warfare might be occurring in IAC or NIAC. According to Additional Protocol I cyber-attack can be constituted as an attack under IHL. There is no question that IHL applies. Principle and rules are aiming to limit the attack that might cause danger to civilian properties and civilian life. As we have seen, using cyber operations in armed conflict can have a serious effect, especially if done in a way that violates IHL.

In particular, IHL noted that civilian and military objects could and must be distinguished in armed conflict. Moreover, the attack itself must be proportionate, and precaution must be given. Following the worldwide cyber-attack, States have been obliged to reconsider their respective cyber-strategies. It is only a matter of time before worldwide cyber warfare breaks out.

BIBLIOGRAPHY


Geneva Convention Relative To The Protection of Civilian Persons, 163.


Protocols Additional to the Geneva Conventions of 12 August 1949, 30.


