Palacký University in Olomouc
Faculty of Law

Can cyber-attacks trigger the right to self-defence under Article 51 of the Charter of United Nations?

Master Thesis

Tram Anh Nguyen **2022**

Palacký University in Olomouc
Faculty of Law

Tram Anh Nguyen

Can cyber-attacks trigger the right to self-defence under Article 51 of the Charter of United Nations?

Master Thesis

Olomouc 2022

Affidavit

I hereby declare that this Master's Thesis on the topic of 'Can cyber-attacks trigger the right to self-defence under Article 51 of the Charter of United Nations?' is my original work and I have acknowledged all sources used.

In Olomouc on 30 June 2022

Tram Anh Nguyen

Acknowledgment

I would like to thank my supervisor JUDr Martin Faix, Ph.D., MJI for his advice and my family for their support throughout the studies.

Table of Contents

List of Abbreviations

ADF	Allied Democratic Forces
CNA	Computer Network Attacks
CND	Cyber Network Defence
CNE	Computer Network Exploitation
CPS	Cyber physical system
CrySyS	Cryptography and System Security
DDoS	Distributed Denial of Service
DNS	Data Name Servers
DoS	Denial of Service
DRC	Democratic Republic of the Congo
ICJ	International Court of Justice
LOAC	Law of Armed Conflict
NATO	North Atlantic Treaty Organization
NCI	National critical infrastructure
PKK	Kurdish Workers' Party
UN	United Nations
UNSC	United Nations Security Council
US	United State of America

INTRODUCTION

Global digitalization is becoming extensive in the twenty-first century and "fostering the rise of social media and other interactive"[1]. A digital revolution makes it possible for an unlimited number of people to stay online everywhere, all the time in an unrestricted way. Alongside the significant benefits of digital technology advancement, many vulnerabilities were introduced by cyber attacks. A well-known example is cyber attack against Estonia in 2007 or the Stuxnet attack against Iran in 2010. In the spring of 2007, Estonia faced a cyber attack campaign (Distributed Denial of Service (DDoS)) lasting a total of 22 days. The attacks were part of a wider political conflict between Estonia and Russia over the relocation of a Soviet-era monument in Tallinn. It paralised the government websites and then infected TV stations, banks, newspapers and other targets[2] but there was no material damage, injuries or loss of life[3]. Stuxnet, a computer worm which is widely believed to have been developed by the United States and Israel, was discovered in 2010 after it was used to attack an uranium enrichment facility at Natanz, Iran. It was the first publicly known use of malicious software designed to cause physical loss or destruction to property by attacking the Supervisory Control and Data Acquisition system of a national critical infrastructure (NCI)[4]. Reports of a threat in early April, 2011, known as DuQu, show that it appeared very similar to the Stuxnet worm in 2010. It has been found in numerous countries, which are France, Netherlands, Switzerland, Ukraine, India, Iran, Sudan, Vietnam. The research carried out by the Laboratory of Cryptography and System Security (CrySyS)[5] showed that the purpose of DuQu was to gather intelligence data and assets from entities such as industrial infrastructure and system manufacturers in order to set up a future attack on various industries, including industrial control system facilities[6].

Today, rapid changes occur in the way international conflict is conducted. A new level of cyber attacks against several governments has potentially spilled into armed conflict. In 2013, Israeli governmental websites were under cyber attacks by the activist group "Anonymous". The group called the attacks "#OpIsrael", and within several hours they were

[1] https://www.bbvaopenmind.com/en/articles/internet-changed-everyday-life/
[2] TIKK, Eneken et al. International Cyber Incidents. Legal Considerations, 2010, p.18.
[3] WATT, Sean M. Low –Intensity Computer Network Attack and Self-Defense. International Law Studies 87, 2011, p.70.
[4] ROSCINI, Marco. Identifying the Problem and the Appicable Law. Cyber Operations and the Use of Force in International Law. Offord: Offord University Press, 2014. p.6
[5] The Department of Networked Systems and Services at the Budapest University of Technology and Economic.
[6] CHIEN Eric at al. W32.DuQu – The Precursor to the Next Stuxnet. Version 1.4. Symantec, 2011, p.1.

claiming to have successfully taken down a large number of Israeli military and government websites. The hackers also published a list of credit card numbers and email addresses apparently lifted from the website of a business selling equipment to the Israeli military[7]. However, the government denied that the actions had caused significant damage to Israel's online infrastructure. Recently, this group has declared a "cyber war" against Russia and its president, Vladimir Putin after Russia invaded Ukraine at the end of February 2022. Since then, the group has claimed responsibility for taking down several websites and leaking data from Russian government agencies[8].

The above list of incidents partly demonstrates new challenges raised by activities in cyberspace. Cyber-attacks pose difficult legal problems with respect to the UN Charter and use of force norms whereas the international legality of cyber warfare remains unsettled. The challenge is that many cyber attacks do not manifest physical damage and the nature of cyber-attacks differs from general armed attacks. It leads to the question of whether cyber attacks can trigger the right to exercise self-defense under Article 51 of the UN Charter.

1. Scope of the thesis

This thesis will not deal with international criminal law, intellectual property, private international law. Also, it does not cross the line of domestic law related to cyber terrorism or cyber crime. The application of human rights law, diplomatic law, law of the sea, air law or outer-space law will not fall within the scope of this research. Instead, the scope of this thesis will be limited to only examining how public international law applies to cyber attacks in peaceful time, i.e. the *jus ad bellum* regime. The further situation of *jus in bello* will not be mentioned in below analysis.

The scope is not limited to the use of cyber force by one state against another state, rather it extends to the matter of non-state actors within the *jus ad bellum* paradigm. Moreover, the details of State resposibility and its attribution will not be discussed in depth. The thesis is focusing on the right of victim State to exercise self-defence if it is under cyber attack according to Article 51 of the UN Charter. Assumptions made in this thesis are that cyber attacks may constitute a use of force and thus amount to an armed attack.

---

[7] FRY, Maddy. Anonymous Launches New Cyberattack Against Israel [online]. Accessible at https://time.com/51616/anonymous-israel-attack/

[8] HUDDLESTON JR, Tom. What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia [online]. Accessible at https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html

2. Purpose of the research

Cyber network attacks are not just a virtual domain[9], in fact they are currently considered a very new type of warfare, besides four traditional domains including land, sea, air and outer-space[10]. Cyber attacks do not have any similarities or classical nature of kinetic scenarios whereas there are no specific norms, customary principles and State practices that cope with the new threats raised in the question of cyber activities. Although in 2013 there was a great attempt of an international group of experts to crack the fundamental question of whether international law applies to cyber activities by publishing famous "Tallinn Manual on the International Law Applicable to Cyber Warfare". However, the Tallinn 2.0 can only be referred to as a recommended source, not binding one. Therefore, the issue of self-defence is still an open door for scholars who want to find the new light in darkness.

Since the absence of lex lata, a controversial topic has arisen in contemporary international law, which is about self-defence against imminent armed attacks and attacks carried out by non-state authors, even though the problem of self-defence in the context of cyber operations is not really a new riddle among jurisprudence studies. This issue was mentioned by Roscini in 'Cyber Operations and the Use of Force in International Law' or Professor Schmitt in his analysis 'Cyber Operations in International Law: The Use of Force, Collective Security, Self-Defense and Armed Conflicts". Both authors propose that cyber attacks should be qualified as the use of force under the law governing the use of armed force by states in international relations (jus ad bellum). This means there is potential for the State victim to invoke the right of self-defence consonant with Article 51 UN Charter if cyber attacks are ascertained as armed attacks.

This thesis aims to examine some existing approaches and arguments relevant to whether a cyber attack can meet the threshold of an armed attack. If the test shows us the positive answer, then the next step will be determining under which conditions cyber attacks could be invoked by victim state to summon the right of self-defence under Article 51 UN Charter or the victim state can pull the trigger in every circumstance. Furthermore, the right of anticipatory self-defense against an imminent armed attack will be discussed in detail. On the other hand, with the increasing participation of non-state actors in cyber attacks against nation states, the inquiry of whether the traditional LOAC rules apply to such authors cannot be

[9] ROSCINI, Marco. World Wide Warfare: Jus ad bellum and the Use of Cyber Force. Cyber Operations and the Use of Force in International Law. Offord: Offord University Press, 2014. p.86
[10] RID, Thomas, MC BURNEY, Peter. Cyber weapon. RUSI Journal 157, 2012, No.1, p.6.

ignored. The overall goal is to assert that current legal regimes in response to cyber threats should be interpreted and recognized in dynamic way.

3. Methodology

First, it should be noted that this topic is not an entirely new idea because there were many articles and journals relevant to the self-defence and cyber attacks, even books that publish professional reviews. Moreover, the cyber attacks that have already occurred only provide uncertain details and data. For this reason, my thesis will not use empirical method to study the legal system. It shall present analytical approach, which to a large extent is based on desk research. Indeed, the thesis mostly examines critical details proposed by Roscini, Schmitt, Dinstein, Corten to add a new conclusion.

Second, the descriptive approach will assist in exploring the concept of terminologies, such as “cyber attack”, “cyber network attack”, “cyber operation” and “cyber warfare” which were developed by legal scholars. Due to the multiplicity of terms, the thesis also incorporates a comparative approach to distinguish “cyber attacks” with different types of cyber activities or multiple sorts of kinetic attacks.

Besides, my thesis will rely on some judgments of ICJ for the purpose of defining what armed attack is, thereby understanding the problem of identifying the author of cyber attacks. As such, by using the normative approach in this situation, the thesis can evaluate the nature of the armed attack and its characteristic in comparison to cyber attacks.

4. Structure

Based upon the application of different methods and topics covered, the thesis is divided into three chapters, which eventually answer the central question of the thesis: Whether cyber-attacks can lay a ground for the exercise of self-defence? This thesis examines these questions and in the process, offers new insights into how Article 51 may be applied to meet the difficulties posed by cyber-attacks.

The first chapter will take a quick look at the prohibition of use of force in contemporary public international law. It is because the scope of ‘force’ in Article 2(4) UN Charter will be used to explain the distinction between the most grave forms and the less grave forms of the use of force.

The second chapter introduces the right of self-defence embedded in Article 51 UN Charter as an exception to the prohibition of the threat or use of force. This part aims to provide the basic knowledge of why the right of self-defence exists besides Article 2(4) UN Charter. The main part of this chapter points out the scope and pre-conditions when a state wishes to trigger the inherent right of self-defence.

The third chapter clarifies what cyber attacks are and explains the unique setting of cyber-attacks. On that basis, we also point out the difference between cyber attacks and other relevant terms, such as cyber exploitation. This part will highlight the concepts, the characteristics from broader category to narrow meaning of computer network as a weapon in the context of cyber operation.

The last chapter will turn to examine whether the victim state might claim the right to self-defence under Article 51 UN Charter when that state is cyber attacked. To answer this difficult question, this part will consider the source of cyber attacks, the categorization of attacks as uses of force and whether cyber attacks can rise to the level of armed attack under the jus ad bellum. Some common approaches will be presented and reviewed in this part.

CHAPTER 1

PROHIBITION OF THE USE OF FORCE

The purpose of this chapter is to seek to expose some focused discussion on the meaning of 'force'. Needless to say, the concept of 'force' is relevant to 'armed attack', 'acts of aggression' as found in some provisions of the Charter but they are not identical. The distinction is significant since, under Article 51, a forcible response in self-defense is only permissible in the event of a 'armed attack'. That means not every use of force contrary to Article 2(4) may be responded to with self-defence.

The prohibition of the threat and the use of force is fundamental in international law. The principle of the prohibition of the threat and the use of force is enshrined in Article 2(4) of the UN Charter. The provision directs that:

> *All Members [of the United Nations] shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations*[11].

This provision is generally considered to represent and reflect existing customary international law and, at least with regard to its core, also *jus cogens.* Accordingly, not only the actual use of force but also the mere threat of force in general is prohibited.

1.1. Scope of the prohibition of 'force'

Article 2(4) prohibits both the threat and the use of 'force' without defining what 'force' is. In other words, the UN Charter gives no guidance when it comes to determining what constitutes a "use of force". Neither treaty nor customary provides an official definition of 'force' or 'threat of force'. Interestingly, the word 'force' appears in the Charter's Preamble, as well as in Articles 41 and 46, where it is followed by the adjective 'armed', whereas only Article 44 clearly means 'armed force'. One point that article 2(4) does not use the adjective 'armed' before 'force'. This has led to an extensive debate whether the term

[11] Article 2, paragraph 4, Charter of the United Nation.

'force' in article 2(4) was meant only 'armed force' or rather to extend to other forms of force, for example, economic coercion.

Traditionally, some commentators insist that 'force' in the context of Charter is limited to 'armed force' even though the reference to "armed force" was not done in Article 2(4)[12]. By contrast, the opposite opinion is in favour of wider notion of 'force'. Some scholars claimed that the concept of force encompasses any illegal action by a state that violates the interests of another, not just armed force[13]. Admittedly, the actual wording of Article 2(4) does not provide clear solution to this dispute. The dominant view, however, is likely reinforced by a teleological interpretation of Article 2(4): if this provision were to extend to other types of force, states would be left with no means of putting pressure on other states that violate international law. Finally, the preamble to the Charter demonstrates that the prohibition of the use of force is exclusively concerned with military force. This conclusion is so far confirmed by the 1970 Declaration on Friendly Relations[14] and followed by the 1974 Declaration on the Definition of Aggression[15] as well as the 1987 Declaration on the Non-Use of Force[16]. These documents underline the fact that the scope of Article 2(4) UN Charter is restricted to 'armed force'. In addition, the preamble of the Charter refers to the need to ensure that 'armed force' should not be used except in the common interest and article 51, dealing with the right to self-defence, specifically refers to armed force but it is not itself conclusive as to the permissibility of other forms of coercion[17].

Despite the lack of clarity regarding the scope of Article 2 (4) UN Charter, a generally accepted understanding is that the term "force" must be denoted "armed"force[18]. Thus we are reluctant to conclude that economic, political or psychological pressure fall within the scope of this provision.

An act does not have to be direct to be considered a use of force because in some cases it might be indirect, such as one State can send mercenaries or give assistance to rebels who

---

[12] A. Randelzhofer and O. Dörr, 'Article 2 (4)', in The Charter of the United Nations, edited by Simma, Khan, Nolte, and Paulus, Vol I, p 209.
[13] KELSEN, Hans. Collective Security Under International Law. U.S. Naval War College: Newport, 1954, vol.XLIX, pp. 55- 57.
[14] Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, GA Res 2625 (XXV), 24 October 1970.
[15] Declaration on the Definition of Aggression, GA Res 3314 (XXIX), 14 December 1974.
[16] Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, GA Res 42/22, 18 November 1987.
[17] SHAW, Malcolm N. International Law. Cambridge University Press, 2008, pp.1124-1128.
[18] FAIX, Martin. Law of Armed Conflict and the Use of Force. Palacky University, 2014, vol I, p.17.

perpetrate acts of violence in another State's territory. The notion of 'indirect force', often imprecisely replaced by 'indirect aggression' refers to the participation of one State in the use of force by another State (e.g. by allowing parts of its own territory to be used for violent acts against a third State), as well as to a State's participation in the use of force by unofficial bands organized in a military manner, such as irregulars, mercenaries or rebels[19]. This notion was confirmed in the case Nicaragua in which the ICJ found that the arming and the training of the contras can certainly be said to involve the threat or use of force against Nicaragua whereas the mere supply of funds to the contras does not in itself amount to a use of force[20]. According to ICJ, use of force can be 'either in the direct form of military action, or in the direct form of support for subversive or terrorist armed activities within another State'. Nonetheless, the ICJ did not provide any criteria by which it could be determined what actions of aid, under what circumstances, are to be constituted a threat or use of force. Overall, it appears that the use of force is an expansive concept, encompassing both the direct and indirect armed force against another state.

The importance in Nicaragua case is in a controversial finding where the Court sub-classified the use of force into most grave forms of the use of force and other less grave forms of the use of force. The most grave forms of use of force are those constituting an armed attack. The acts that involve a threat or use of force, such as organizing, instigating, assisting, or participating in acts of civil strife and terrorist acts in another State, but not amounting to an armed attack can be classed as the less grave forms of the use of force.

1.2. The exceptions of the prohibition on the use of force

As indicated above, the very broad scope of the Article 2(4) prohibition must in particular be read in conjunction with Chapter VII of the Charter, which legitimizes two types of action involving the use of force: actions taken as part of collective security operations pursuant to Chapter VII and actions taken in self-defense as laid down in Article 51. Those are also only two important exemptions of Article 2(4).

The first exception to the general prohibition of the use of force falls under Article 39 of the UN Charter or the so-called 'collective security' mechanism. Article 39 grants the

[19] SIMMA, Bruno, MOSLER, Hermann et al.The Charter of the United Nations: A Commentary, 2rd edition. Oxford University Press, 2013, p.119.
[20] Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Judgment of 26 November 1984, ICJ, paragraph 228.

Security Council authority to 'determine the existence of any threat to the peace, breach of the peace, or act of aggression, and to make recommendations, or decide what measures shall be taken to maintain or restore international peace and security'[21]. In light of the above, if the UN Security Council considers the aforementioned measures inadequate for maintaining or restoring international peace and security, it may decide on measures that shall be taken, in accordance with Articles 41 (non-forcible measures) or 42 (forcible measures), in order to maintain or restore international peace and security.

The second exception to to the general prohibition of the use of force is codified in Article 51, which permits States to make such determinations and take such measures until the Security Council takes its own measures to maintain international peace and security. In other words, it is the right of states to act, on their own initiative, in self-defence. The right of self-defence laid down in Article 51 of the UN Charter, being the only exception to the prohibition of force of practical significance, has therefore become the pivotal point around which disputes concerning the lawfulness of the use of force turn. However, there is restriction in the sense of Article 51, which intends to prevent unnecessary escalation of armed conflicts between states. Only if the prohibited use of unlawful force rises to an armed attack can states use forcible measures for its defense. It should be emphasized that with respect to the use of force, there is a discrepancy of scope between the prohibition of 'force' under article 2(4) and the exception in case of 'armed attack' of article 51 of the UN Charter. This gap will be discussed further in the next Chapter.

[21] Article 39, Charter of the United Nations.

CHAPTER 2

THE RIGHT TO SELF-DEFENCE

This chapter will deal with the law of self-defence, probably the most controversial area of the *jus ad bellum.* The purpose is seeking the doctrinal conclusion about the meaning of 'armed attack' in Article 51 UN Charter, because the legal ground for the right of individual and collective defense is occurrence of an 'armed attack'. Moreover, this part will dig deeper into the legal bond between the scope of Articles 2(4) and 51 respectively, arguing that not all violations of Article2 (4) will necessarily amount to an 'armed attack', thus justifying a lawful, forcible self-defense response under Article 51.

2.1. General overview

The right of self-defence is enshrined in Article 51 of the Charter of the United Nations, which reads as follow:

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.* [22]

The International Court of Justice in the Nicaragua case clearly established that the right of self-defence existed as an inherent right under both customary international and the UN Charter. It was emphasised that:

> *Article 51 of the Charter is only meaningful on the basis that there is a 'natural' or 'inherent' right of self-defence and it is hard to see how this can be other than of a customary nature, even if its present content has been confirmed and*

[22] Article 51, The Charter of United Nation

influenced by the Charter . . . It cannot, therefore, be held that article 51 is a provision which 'subsumes and supervenes' customary international law.

Accordingly, customary law coexisted with treaty law (i.e. the UN Charter) in this sphere. Consequently, the rules did not have the exactly same content and they did not overlap.

This Article should be considered together with Article 2(4) UN Charter, which requires states to refrain not only from the use of force but also from the threat of use of force. This principle, however, is subject to two exceptions, which may allow Member States to use force in the event of an armed attack: individual and collective self defense. Article 51 hence speaks of both "individual" and "collective" self-defence.

2.2. The nature of self-defense in Article 51 of UN Charter

2.2.1. The inherent right

Needless to say, individual self-defence at first is a right, not an obligation[23]. Indeed, international law does not set down any duty to resort to self-defence. Practically, should an armed attack occur a target state is free to exercise or to refuse to exercise this right[24]. On the other hand, one question was raised relevant to the second form of self-defense. Is the exercise of collective defense merely a right same as individual defense? Assuming that a state or states are bound by regional or mutual assistance treaties they are under a duty to act, imposed by particular international law. A good example that can be mentioned is an international treaty that establishes a military alliance. In this case, mutual assistance to another state is required, and it may include legal obligation to collective self-defense. Hence, this form of obligation must be read carefully within the context of 'unit' self-defense.[25]

The feature of self-defense also raises thorny questions regarding whether or not this concept carries a resemblance to 'self-help' because the two terms were sometimes used interchangeably. The early scholars regard the concepts of self-help and self-defence as linked but distinct, notably Krift in his article concluded that 'whereas self-defense is directed

[23] DINSTEIN, Yoram. War, Agression amd Self-Defence. 6th edition. Cambridge: Cambridge University Press, 2017, pp.175-218
[24] FAIX, Martin. Law of Armed Conflict and the Use of Force. Palacky University, 2014, vol I, pp. 61-87
[25] DINSTEIN, Yoram. War, Agression amd Self-Defence. 6th edition. Cambridge: Cambridge University Press, 2017, pp.175-218

against actions of other States, self-help is directed against actions not attributable to States'[26]. On the same line, Prof. Linnen agrees that 'self-preservation and self-help under eighteenth and nineteenth century views of the law of nations are predecessors of modern self-defense, but differ from it in significant respects'[27]. In different approaches, self-defence is determined as "a lawful form of self-help against a specific violation of international law"[28]. Similarly, the modern authors confirm this comment from the point of view that the essence of self-defence has its root in self-help[29] or that self-defence is a manifestation of "armed self-help". Modern approach seems to be more reasonable and flexible because self-help under international law comes in different varieties, ranging from retorsion, reprisals, self-preservation or (self-protection) to self-defense itself. In other words, self-defence like the lawful application of a sanction are permitted forms of self-help, and not concepts that are distinct from, although somewhat similar to, it[30].

2.2.2. A temporal right

The fact is that the right of self-defence guaranteed by Article 51 UN Charter has a temporal scope. First, states must immediately report to the Council any self-defense measures that they employ, otherwise those measures are considered unlawful. Furthermore, the second phrase of Article 51 provides that self-defence measures 'shall not in any way affect the authority and responsibility of the Security Council (…) to take at any time such action as it deems necessary in order to maintain or restore international peace and security'. It means the right to self-defence is only valid until the Security Council has taken measures necessary to secure international peace and security. To put it another way, as soon as the Security Council has adopted such measures, the right to exercise self-defense of the victim state will be ceased. This suggests that the right to self-defence is a temporal solution in case of one state being attacked by another state.

---

[26] KRIFT, Thomas R. Self-Defense and Self-Help: The Israeli Raid on Entebbe. Brooklyn Journal of International Law, 1977, vol. 4, no. 1, pp. 43-62.
[27] LINNAN, David K. Self-defense, Necessity, and U.N collective security: United States and other views. Duke journey of Comparative and International Law, 1991, pp.57-123.
[28] KELSEN, Hans. Collective Security and Collective Self-Defense under the Charter of the United Nations. American journal of international law, 1948, vol. 42, pp. 783–84.
[29] DINSTEIN, Yoram. War, Agression amd Self-Defence. 6th edition. Cambridge: Cambridge University Press, 2017, pp.175-218; FAIX, Martin. Law of Armed Conflict and the Use of Force. Palacky University, 2014, vol I, pp. 61-87.
[30] Report of the International Law Commission. Year book of the International Law Commission, 1980, vol.2, Part one, paragraph 95.

This characteristic of the right to self-defence is designed based on two grounds. Initially, the Security Council has exclusive competence which is 'primary responsibility for the maintenance of international peace and security'[31], meaning the Security Council plays the central role in addressing disputes involving armed force between States. Therefore, the Members of the United Nations must 'accept and carry out the decisions of the Security Council in accordance with the present Charter'[32]. The point that must be noted here is the obligation of the states to show respect before the Security Council. Even if states have already reacted, or are reacting, in individual or collective self-defence, they cannot extend the defensive right since the exercise of self-defence by states becomes unnecessary once the Council takes over. The second reason is that, as previously said, self-defense is only a right, thus it has legal dimensions and judicial processes are not eliminated in consequence of the Council's authority[33].

1.3. The main requirement for the exercise of the right of self-defence

According to the language of Article 51 UN Charter, the right to self-defence arises only if an armed attack occurs. In other words, an armed attack is a prerequisite for a State to resort to the right of self-defense. This is also a central difficulty in applying Article 51. Within the meaning of that expression in Article 51, it is very clear that the use of force in self-defense depends on whether an armed attack occurs or not and the victim state must be able to prove the facts showing its existence[34]. In this regard, the term 'armed attack' represents key notion of the concept of self-defence pursuant to Article 51. This view was reaffirmed by the Eritrea Ethiopia Claims Commission, concluding that:

> *As the text of Article 51 of the Charter makes clear, the predicate for a valid claim of self-defense under the Charter is that the party resorting to force has been subjected to an armed attack.*[35]

[31] Article 24, United Charter
[32] Article 25, United Charter
[33] Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Judgment of 26 November 1984, ICJ, paragraph 98.
[34] Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), ICJ Reports 2003, p.161. In this case, the judgment placed 'the burden of proof of the facts showing the existence' of an armed attack rests on the State justifying its own use of force as self-defense.
[35] ERITREA-ETHIOPIA CLAIMS COMMISSION. Partial Award Jus Ad Bellum-Ethiopia's Claims 1-8. Report of International Arbitral Award, 2005, Vol. XXVI, paragraph 11, p.465.

Yet, the problem of the definition of the term 'armed attack' has not been solved. Neither International Law nor the UN Charter provides precisely what constitutes an armed attack. Instead, the concept of armed attack is reflected in jurisdiction of ICJ, starting with the Nicaragua case. Following the Nicaragua case, series of cases occurred including Oil Platforms, Armed Activities on the Territory of the Congo (DRC v Uganda), and The Legal Consequences of the Construction of a Wall on the Occupied Palestinian Territory. Thus it is necessary to gain a better insight into the notion of 'armed attack' in general.

1.3.1 Definition of 'armed attack'

The UN Charter uses the term 'armed attack' in Article 51 albeit without defining it anywhere. By contrast, the Court in the Nicaragua case took the Assembly Resolution 3314 (XXIX) of 14 December 1974 as a starting point in its analysis of the definition of armed attack. It seemed to equate 'armed attack' to a special form of 'aggression' when it recognized that an armed attack occurs either when regular armed forces cross an international border, or when a state sends 'armed bands, groups, irregulars or mercenaries which carry out acts of armed force against another State of such gravity as to amount to' an actual armed attack by regular forces. However, it does not mean that both notions 'armed attack' and 'aggression' are identical. An act of aggression can constitute an armed attack, but it may not always do so[36]. In legal writing, the view regarding 'armed attack' as the narrower term is dominant. As maintained by Dinstein, 'aggression' is much broader and looser term and therefore 'an "armed attack" is actually a particular type of aggression'[37].

Having in mind that the Nicaragua judgment by the ICJ has not brought about clarification in this respect, on the term 'armed attack' the ICJ simply remarks that 'there appears now to be general agreement on the nature of the acts which can be treated as constituting armed attack'[38]. Instead of providing definition of the term, the ICJ just gives an example to illustrate the existence of an armed attack in the form of 'aggression'.

---

[36] Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 71, pp.339-348.
[37] DINSTEIN, Yoram. Computer Network Attack and Self-Defene. International Law Studies, US. Naval War College, 2002, Vol.76, pp.99-119.
[38] Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Judgment of 27 June 1986, ICJ, paragraph 195.

1.3.2.General factors determining the existence of an 'armed attack'

From the threshold perspective, the armed attack requires the following factors: what acts count as armed attack? (the form), when does an armed attack take place? (scope) and from whom must the armed attack emanate? (the originator)

a) What acts count as armed attack?

It is not so clear whether or not all forms of armed force are equated to an armed attack and whether they could give rise to the exercise of the right to self defense. Thus it becomes necessary to identify the factors that allow us to distinguish between 'armed attack' and other forcible acts not triggering the right to self-defence. In other words, there exists a certain gravity threshold which must be reached before an attack can qualify as 'armed' in the sense of Article 51.

Relevant to this issue, the ICJ found a relationship between the conventional norms 'use of force' and 'armed attack' in Nicaragua judgment on June 27, 1986 although the Court does not concern Article 2(4) and Article 51 directly. In the well-known Nicaragua case, the Court famously and controversially said that 'It is necessary to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less grave forms'[39]. The Court ascertains rules that apply for less grave forms of the use of force by referring to the Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations (General Assembly resolution 2625 (XXV). Accordingly, these rules include: the duty to refrain from the threat or use of force to violate the existing international boundaries; duty to refrain from acts of reprisal involving the use of force; the duty to refrain from any forcible action which deprives peoples referred to in the elaboration of the principle of equal rights and self-determination of that right to self-determination and freedom and independence; the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands; the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts[40]. More importantly, the Court identifies a category of acts which do not in its view constitute armed attack, but is regarded as a threat or use of force (less grave forms of

[39] Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, ICJ, paragraph 51

[40] Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Judgment of 27 June 1986, ICJ, paragraph 191.

the use of force), namely 'assistance to rebels in the form of the provision of weapons or logistical or other support'[41].

At the same time, the Court explained that the difference between 'armed attack' and a less grave form of the use of force is primarily one of 'scale and effects'. Indeed, the Court asserted that 'the prohibition of armed attacks may apply to the sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack'[42]. 'Mere frontier occurrences', on the other hands, do not qualify as an armed attack (unless they reach the sufficient gravity required in armed attacks).

Similar language was found in well-known Oil Platforms case. Particularly, the Court reiterates the boundary between the most grave forms and other less grave forms of the use of force and confirms that only the former can qualify as armed attack[43]. In order to establish that it was legally justified in attacking the Iranian platforms in exercise of the right of individual self-defence, the Court reaffirmed the requirement of how serious an attack must be [44]. The Court did not exclude the possibility that an attack on a single vessel could amount to an armed attack[45]. Nonetheless, the Court determined that the alleged attacks, even taken cumulatively, did not constitute an armed attack, as a most grave form of the use of force[46]. In reaching this conclusion, the Court made statements that might be read as suggesting that the attacks must rise to unspecified level of gravity before they would qualify as armed attacks. Put another word, the use of deadly force by a State's regular armed forces, such as the attacks by Iran at issue in this case, do not qualify as an armed attack unless they reach a certain level of gravity[47].

The distinction between armed attack and other less grave use of force was a crucial question in the Eritrea/Ethiopia Claims Commission Award on Ethiopia's Ius ad Bellum Claims 1–8[48]. The important issue before the tribunal was whether Eritrea had started the

---

[41] Id, paragraph 195.
[42] Id, paragraph 195.
[43] Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, ICJ, paragraph 51.
[44]Id, paragraph 51.
[45] Id, paragraph 72.
[46] Id, paragraph. 64.
[47] TAFT, William. H. Self-Defense and the Oil Platforms Decision. The Yale Journal of International Law, 2004, Vol.29, pp.300-301.
[48] ERITREA-ETHIOPIA CLAIMS COMMISSION. Partial Award Jus Ad Bellum-Ethiopia's Claims 1-8. Report of International Arbitral Award, 2005, Vol. XXVI, pp.457-469.

1998–2000 conflict and should be held responsible for all the harm to Ethiopia caused by that conflict. The parties disagreed as to the starting point of the conflict. Ethiopia claimed that Eritrea carried out a series of unlawful armed attacks against it, beginning on May 12, 1998, in violation of jus ad bellum; whereas Eritrea argued that those actions were lawful measures of self-defence in response to the illegal occupation of Ethiopian forces on its territory and the forcible incursions happened in early May 1998. With respect to the events in the vicinity of Badme that occurred during the period from May 6–12, 1998, the Commission acknowledged the sharply different accounts offered by the Parties as to the precise location of the incidents of May 6 and 7 and the numbers and types of forces involved. However, it had no need to resolve these differences because it is clear from the evidence that these incidents involved geographically limited clashes between small Eritrean and Ethiopian patrols along a remote, unmarked, and disputed border. The Commission was satisfied that these relatively minor incidents were not of a magnitude to constitute an armed attack by either state within the meaning of Article 51 of the UN Charter. Regrettably, no details about how minor the incidents had been were presented. On the other hand, the Commission further concluded in its Partial Award 'Localized border encounters between small infantry units, even those involving the loss of life, do not constitute an armed attack for purposes of the Charter'[49].

As reflected in the jurisdiction of the ICJ, Article 51 and 2(4) do not fully correspond to one another in scope. Rather, the latter constitutes a part of the former because the use of force is not limited to 'armed force' whereas the concept of armed attack necessitates the employment of arms. As a result, not every use of force can be met with the right to exercise self-defense. Furthermore, all the abovementioned cases imply that the use of force has the position below the threshold of an armed attack. ICJ's view clearly shows that not every use of force must be classified as an armed attack, unless it reaches the *de minimis* threshold of gravity. It was supported by the argument that if there is no gravity requirement for an armed attack and self-defence, then an inter-state conflict could arise out of minor cross-border incidents or other minor uses of force[50]. The threshold of an armed attack is degree of force which can be understood as a massive, large-scale attack with substantial effects[51]. It also does not exclude a small-scale attack with sufficient gravity.

[49] Id, paragraph 11.
[50] GRAY, Christine. International Law and the Use of Force. Oxford University Press, 2008, 3rd Edition, p.132.
[51] RANDELZHOFER,Albrecht, NOLTE,Georg. 'Article 51' in Bruno Simma, Hermann Mosler, Andreas Paulus and EleniChaitidou (eds), The Charter of the United Nations: A Commentary, 3rd edition. Oxford University Press, 2013

b) From whom must the armed attack emanate?

States

Regarding the authors of an armed attack, the traditional approaches only recognize that States are territorial subjects based on the concept of sovereignty. This has been the generally accepted interpretation for many years. The jurisprudence of ICJ shows that the Court has been receptive to this approach, adopting a narrow interpretation of 'armed attack'. In its advisory opinion on the case Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, the Court's observations may be read as reflecting the obvious point that:

> *Article 51 of the Charter thus recognizes the existence of an inherent right of self-defence in the case of armed attack by one State against another State.*[52]

As maintained by the Court, Israel could not in any event invoke those resolutions in support of its claim to be exercising a right of self-defence since Israel did not claim that the attack against it was imputable to a foreign State. Consequently, the Court concluded that Article 51 of the Charter has no relevance in this case.

The strict view of ICJ in the Wall case finds its support in the case Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda) in which the Court is of the view that the attacks emanated from armed bands or irregulars remained non-attributable to the State (DRC)[53]. For this reason, the Court found that the justification for the exercise of a right of self-defence by Uganda against the DRC were not present[54]. It seems that the Court chose to follow the classic approach when its decision reaffirmed that:

> *Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these parameters*[55].

---

[52] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, ICJ, paragraph 136.
[53] Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment of 19 December 2005, ICJ, paragraph 146.
[54] Id, paragraph 147.
[55] Id, paragraph 148.

Traditionally, Article 51 solely applies to armed attacks mounted by one State against another. In other words, the use of force in the right of self-defence is only applicable against armed attacks between States.

Another form of armed attack was officially accepted in case of attack by terrorists or members of armed bands who qualify as 'de facto organs' of a State. This stems from states either directing private individuals or groups to conduct unlawful acts or being heavily involved in them, such as offering financial assistance, providing logical support or facilitating base or training field. Those behaviors are prohibited by Public International Law, particularly Resolution 2625, 2734, and 3314 were adopted by the UN General Assembly. All documents declare explicitly that every State has the duty to refrain from organizing, participating, or supporting terrorist acts in another State, and acquiescing in organized activities within its territory direct towards the commission of such acts[56]. Further, State responsibility can not be excluded from the circumstance that a State fails to take reasonably available measures to stop such acts in breach of its obligations to other states[57]. According to the judgment in the Corfu Channel case of 1949, the ICJ draws the conclusion that every State is under an obligation 'not to allow knowingly its territory to be used for acts contrary to the rights of other State'[58]

Non-state entities

It is clear that the right of self-defence applies to armed attacks by other states, the question has been turned to whether the right of self-defence applies in response to attacks by non-state entities. In Armed Activities on the Territory of the Congo (DRC v Uganda) case, the DRC brought an action against Uganda for unlawful use of force. Uganda attempted to justify its use of force by claiming self-defense. To support its claim, Uganda accepted a broad view of armed attack that the DRC bears responsibility for attacks by the irregular forces of the Allied Democratic Forces (ADF) operating from the DRC against Uganda. In particular, Uganda claimed that the ADF, a rebel group operating against Uganda from Congolese territory, was being supplied and equipped by the Sudan and the DRC government. However, Uganda made no claim to having been attacked by the DRC's armed forces and the subject of armed attacks was ADF. The argument was mainly about the involvement of DRC in these

[56] Resolution adopted on the Reports of the Six Committee, General Assembly. Accessible at https://treaties.un.org/doc/source/docs/A_RES_2625-Eng.pdf

[57] According to Article 11 of Draft Articles on State Responsibility, conduct is attributable to a state as under its control if "*the State acknowledges and adopts the conduct in question as its own*."

[58] The Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ, p.22.

attacks but the Court did not find satisfactory proof relevant to this claim. Moreover, the Court did not answer the questions whether there may be an armed attack by non-state actors in the absence of substantial involvement of the state, and what measures a state may take against such an attack. The ICJ concluded that:

> *Accordingly, the Court has no need to respond to the contentions of the Parties as to whether and under what conditions contemporary international law provides for a right of selfdefence against large-scale attacks by irregular forces.*[59]

Contrary to classic views, some scholars have attempt to formulate a new approach to the concept of self-defence when they extend the subject of an armed attack to non-State actors. Judge Higgins in her Separate Opinion does not agree with all that the Court has to say on the question of the law of self-defence.

> *There is, with respect, nothing in the text of Article 51 that thus stipulates that self-defence is available only when an armed attack is made by a State.*[60]

Similar arguments were presented by Judge Kooijmans when he refers to Resolutions 1368 (2001) and 1373 (2001) which both recognize the inherent right of individual or collective self-defence without making any reference to an armed attack by a State[61]. It seems probable that the above explanation is to be found in the similar comment of Murphy. He contends that the language used in Article 2(4) (which speaks of a use of force by one 'Member' against 'any state') is not repeated in Article 51, hence, the originator of armed attack is not necessarily identified as a State[62]. However, it should be mentioned that we are discussing the context of an armed attack mounted by a non-state actor operating from a foreign state[63] and which is not sponsored by the State (not de facto organ or agent). A very famous example is the lethal attack against the US on 9/11 carried out by Al-Qaeda terrorist organization. The terrorists hijacked four airliners and flew three of the planes into buildings:

---

[59] Case concerning Armed activities on the territory of the Congo (Democratic Republic of the Congo v.Uganda), Judgment of 19 December 2005, ICJ, paragraph 147.
[60] Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Separate Opinion of Jugde Higgins, ICJ, paragraph 33.
[61] Id, Separate Opinion of Judge Kooijmans, ICJ, paragraph 35.
[62] MURPHY, Sean D. Terrorism and the Concept of Armed Attack in Article 51 of the U.N.Charter. Harvard International Law Journal, 2002, vol. 43, no. 1, pp. 41-52.
[63] It should be distinguish to the scenario on which non-State actors attack a State from within its teritory and no other State is involved. This is a case of either an internal armed conflict or domestic terrorism.

the twin towers of the World Trade Center in New York and the Pentagon in Arlington, Virginia, causing 2,976 death and thousands more injured. The question is whether terrorist acts have a sufficient degree to meet the requirements of armed attacks when the terrorist attacks come from outside of the control of any state.

The horrifying terrorist attacks which took place on 9/11/2001 in the US were unequivocally condemned in Resolution 1368 (2001) of the Security Council which affirms that such an act of international terrorism is a threat to international peace and security[64]. Moreover, Resolution 1368 also refers in its preamble the inherent right of individual or collective self-defence of a State to respond to terrorist attacks in accordance with the Charter[65]. It means the right of self-defence against an armed attack by non-State actors without substantial involvement of a State has met widespread acceptance, especially by modern scholars[66]. As claimed by Gray, Resolution 1368 shows the willingness of Member States to accept legal applicability of the right of self-defence against terrorist attacks. Professor Schmitt also emphasized that:

> *[…]states seem comfortable with applying the concept of armed attacks to situations involving non-state actors. Should such groups launch cyber attacks meeting the threshold criteria for an armed attack, states would likely respond within the framework of the law of self-defense.*[67]

On this matter, it is reasonable to make a reference to the Chatham House Principles of 2005 because the wording suggests that Article 51 is not confined to self-defence in response to attacks by states. In addition, the right of self-defence *'*is a right to use force to avert an attack. The source of the attack, whether a state or a non-state actor, is irrelevant to the existence of the right'.[68] In summary, it is now accepted that a non-state actor can mount an armed attack but the attack is necessarily launched from foreign state.

c) When does an armed attack take place?

---

[64] Resolution 1368 (2001) adopted by the Security Council at its 4370th meeting, on 12 September 2001.
[65] Id
[66] DINSTEIN, Yoram. War, Agression amd Self-Defence. 6th edition. Cambridge: Cambridge University Press, 2017, pp.175-218; MURPHY, Sean D. Terrorism and the Concept of Armed Attack in Article 51 of the U.N.Charter. Harvard International Law Journal, 2002, vol. 43, no. 1, pp. 41-52; GRAY, Christine. International Law and the Use of Force. 3rd edition. Oxford University Press, 2008, p.202
[67] SCHMITT, Michael N. Cyber Operations and the *jus ad bellum* Revisited. Villanova Law Review, 2011, pp.569-606.
[68] Principle of International Law on the Use of Force by States in self-defence, Chatham House, 2005.

Dealing with this topic, this section will seek the answer referring to the doctrine related to anticipatory self-defence, one of the most controversial questions in contemporary international law. In other words, the question is whether a state must wait until it is attacked before it can respond in self-defence or whether it is entitled to pre-empt an attack.

The vast majority of legal scholars agree that under the literal reading of Article 51 the right to self-defence can be resorted to only if an armed attack has in fact occurred. Among them, some States (US, UK and Israel)[69] and scholars also strongly support the view that anticipatory action in self-defence can be lawful. This group believes that States need not necessarily await the occurrence of an armed attack (no need to wait for the bombs to fall or fire to open because otherwise it would be too late to effectively repel the attack[70]). Nevertheless, this right is limited to 'imminent threats' of armed attack which were formulated in pre-customary "Caroline incident'[71]. In respect of Caroline case, Webster's famous formula suggests that in order to justify anticipatory self-defense a state must demonstrate 'the necessity of that self-defense is instant, overwhelming and leaving no choice of means, and no moment for deliberation.'[72] This definition accepts the extension of the right to self-defence because it did not require an actual armed attack[73]. The legal justification for anticipatory self-defence basically based on the immediacy requirement. The immediacy requirement takes into consideration the amount of time between the threat of an attack and the use of force response thereto[74]. Regarding the imminence of the threat, one question must be raised as to how close in time must the threat of an attack be to the response in order to be considered immediate?

Since self-defense pursuant to Article 51 UN Charter has a strong connection with armed attack, it is critical to pinpoint the precise moment when the armed attack begins. Currently, there is no consensus among states or in legal doctrine about when the right to self-defense arises or when does an armed attack take place[75]. Dinstein suggested that an armed attack can take place at an incipient stage even if it has not yet fully developed in its

[69] GRAY, Christine. International Law and the Use of Force. Oxford University Press, 2008, 3rd Edition, p.141.
[70] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.79.
[71] RUYS, Tom. Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practice. Cambridge: Cambridge University Press, 2010, pp. 255-256.
[72] COHAN, John Alan. The Bush Doctrine and the Emerging Norm of Anticipatory Self-Defense in Customary International Law. Pace International Law Review, 2003, p.328.
[73] VAN DE HOLE, Leo. Anticipatory Self-Defence Under International Law. American University International Law Review 19, 2003, no. 1, p.97.
[74] Id, p.329
[75] RANDELZHOFER, Albrecht. The Charter of the United Nations, a commentary, edited by Bruno Simmma, 3rd edition, volume I. Oxford University Press, 2012, p.1421.

consequences[76]. To be precise, he pointed out three hypothetical Pearl Harbor events scenarios, assuming that that the Americans knew exactly what the Japanese were up to. The easiest scenario relates to the hypothetical shooting down by the Americans of the incoming Japanese aircraft in the relatively short timeframe between launch from the air carriers and the actual execution of the attack mission[77]. He concludes that once the launch was completed, the Japanese armed attack has begun. The more difficult hypothesis concerns the Japanese fleet, which has been destined in mid-ocean in preparation for the attack on Pearl Harbor. If Americans, perhaps by breaking Japanese naval codes, had got convincing evidence about the aim of the navy mission, then Japanese armed attack may be said to have begun to occur[78]. The last situation is the Americans sought to destroy the Japanese fleet before it sailed while it was still training for its mission, war-gaming or otherwise making advance preparations. However, according to Dinstein these actions cannot be seen as crossing the red line of an armed attack[79]. The point is the temporal scope of an armed attack can be counted at the moment it become evident to the victim State that the attack is actually in being progress of being mounted.

In reality, we can carefully assess a series of events in the typical example, namely 'Six-Day War' of June 1967. Israel invoked the right to self-defence in response to an incipient armed attack by Egypt (later joined by Jordan and Syria). Israel argues that when all of the measures taken by Egypt (especially the closure of the Straits of Tiran; the peremptory ejection of the United Nations Emergency Force from the Sinai Peninsula and the Gaza Strip; the unprecedented build-up of Egyptian forces along Israel's borders; and constant sabre-rattling statements about the impending fighting) were weighed cumulatively, it seemed to be obvious that an Egyptian armed attack was in progress. It is safer to argue that, if Israel had reacted to the massing of troops at its border by its Arab neighbours and to the blockade of the Strait of Tiran not by bombing the Egyptian air force but by incapacitating Egypt's air force radars and command and control systems with a massive cyber attack, the legality of such attack would have probably not been doubted[80].

[76] DINSTEIN, Yoram. War, Agression amd Self-Defence. 5th edition. Cambridge University Press, 2011, p.200.
[77] Id, p.204.
[78] Id,p.204.
[79] Id, p.204.
[80] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.79.

CHAPTER 3

CYBER ATTACKS

It is hardly surprising that cyber attacks have become a general concern of international community, especially when several states have been the target of them. Nowadays, cyber attacks have certain distinct qualities that set them apart from the traditional, physical, kinetic battlefield. Understanding those characteristics is moving one step forward toward identifying the challenges that cyber attacks pose to the norm of *jus ad bellum,* because in the world of kinetic combat, those features are non-existent. To put it another way,

it is essential to identify and specify different types of cyber attacks in order to determine the legal regime applicable in the context of cyber attacks. Thus, this part first seeks to provide a comprehensive definition of "cyber attack" on the ground of existing approaches. This step is necessary because it serves to clarify the nature of modern cyber attack or what it is meant to include and exclude. It is very imperative in applying *jus ad bellum* threshold to them.

3.1. Definition of cyber attacks

The definition of 'cyber attacks' is critical for determining how cyber attacks are treated under international law. It should be noted that there are no precise and universal definitions in this domain. Scholars frequently use the phrase 'cyber warfare'[81], 'cyber operations'[82], 'cyber threats'[83], 'computer network attack'[84], 'information operation'[85] interchangeably with the term 'cyber attacks'. Still, the definition of cyber attack is challenged and questioned. However, the definitional ambiguity of cyber attack has not deterred academia, military, or governments in attempting a definition. Currently, the literature on cyber attack indicates two distinct interpretations of the term: some refer to computers and networks as attack targets (the target-based approach), whilst others refer to the use of computers and computer networks as attack instruments (the instrument-based approach). After describing some existing conceptions, a definition that effectively encompasses the issues raised by cyber-attacks in *jus ad bellum* will be offered.

3.1.1. The target or objective - based approach

In 2006, the U.S. Army's Cyber Operations and Cyber Terrorism Handbook used the term 'cyber attacks', defining it as:

> *The premeditated use of disruptive activities, or the threat thereof, against computers and/or networks, with the intention to cause harm or to further social,*

[81] CLARKE, Richard A, KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It, 2010, 320p.
[82] SCHMITT, Michael N. Cyber Operations and the Jud Ad Bellum Revisited. Villanova University, 2006, Vol.56, Issue 3, pp. 569-605.
[83] BRENNER, Susan W. Cyberthreats: The Emerging Fault Lines of the Nation State. 1st Edition. Oxford University Press, 2009, 320p.
[84] SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 1999, pp 886-937.
[85] HOLLIS, Duncan B. Why State need an informational Law for Information Operations. Lewis & Clark Law Review, 2007, Vol. 11, pp.1023 – 1061.

ideological, religious, political or similar objectives. Or to intimidate any person in furtherance of such objectives.[86]

In the 2009 report on U.S. cyber attack capabilities, the U.S. National Research Council defined cyber attack as 'the use of deliberate actions - perhaps over an extended period of time - to alter, degrade, or destroy adversary computer systems or networks and/or programs resident in or transiting these system or network'[87]. Along the same vein, Hathaway recommends a definition which, according to her, focuses attention on the unique threat posed by cyber-technologies[88]:

A cyber-attack consists of any action taken to undermine the functions of a computer network for a political or national security purpose.[89]

Similarly, Clarke defines cyber-war as 'actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption'[90].

This model has received a lot of criticism because it seems to focus on computer systems or networks as the target of an attack carried out by any methods. It leads to a consequence that any means (such as: hacking, bombing, cutting, infecting, and so forth) may be used to accomplish a cyber attack. As a result, those definitions are highly susceptible to an overly wide application of the war framework in the context of cyberspace. In addition, the interpretation of Clark and Hathaway is inadequate, particularly for assessing the legality of modern cyber attack.[91] Instead of characterizing the mode of the attack, Clark and Hathaway refer to "cyber" as the object of the attack (for example, "actions taken to disrupt or destroy computer networks"), which seems to be outdated in favour of more fashionable prefix "cyber". For instance, Stuxnet was not employed in order to destroy the computer, rather it treats the target computer as a channel for an attack on a different target[92].

---

[86] U.S. ARMY TRAINING & DOCTRINE COMMAND. Critical Infrastructure Threats and Terrorism. DCSINT Handbook No. 1.02, 2006, VII-2.
[87] NATIONAL RESEARCH COUNCIL. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington. DC: The National Academies Press, 2009, 360p.
[88] HATHAWAY, Oona A. et al. The Law of Cyber - Attack. California Law Review, 2012, Vol.100, pp.817-885
[89] Id
[90] CLARKE, Richard A, KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It, 2010, 320p.
[91] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129.
[92] Id

In 2011, after establishing the United States Cyber Command, the Joint Chief of Staff of the US proposed a more limited concept of cyber attack in a lexicon for military use in cyber operations. It is quoted as follows:

> *A hostile act using computer or related networks or systems, and intended to disrupt and/ or destroy an adversary's critical cyber systems, assets, or functions. The intended effects of cyber attack are not necessarily limited to the targeted computer systems or data themselves-for instance, attacks on computer systems which are intended to degrade or destroy infrastructure or C2 capability. A cyber attack may use intermediate delivery vehicles including peripheral devices, electronic transmitters, embedded code, or human operators. The activation or effect of a cyber attack may be widely separated temporally and geographically from the delivery.*[93]

Based on the objective of the attack, this definition makes effort to restrict cyber attacks to hostile conduct using computer or related networks or systems that are intended to harm critical cyber systems[94], thus the scope of cyber attack is narrower than the previous one. Nevertheless, the language used in this context does not show the difference between a cyber-crime, cyber-attack, and cyber-war, leading to broad interpretations.

3.1.2. The instrument - based approach

Unlike the model that looks at the target of attacks, the second approach concentrates on the method of delivery. A cyber attack, according to this view, can be an instrument, method, or capability that is employed to achieve a specific goal. Thus, the term "cyber attack" commonly refers to the employment of cyber operations as a weapon or form of attack, wherein the central factor -"cyber" - connotes the method to conduct an attack[95].

The most famous definition of 'cyber attack' under an instrument – based approach is probably that of Shanghai Cooperation Organization, which describes it as 'the threats posed by possible use of [new information and communication] technologies and means for the

[93] Memorandum for Chiefs of the Military Services, Commanders of the Combatant Commands, Directors of the Joint Staff Directories, 2011
[94] HATHAWAY, Oona A. et al. The Law of Cyber - Attack. California Law Review, 2012, Vol.100, pp.817-885
[95] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129

purposes [sic] incompatible with ensuring international security and stability in both civil and military spheres.'[96]

The Shanghai Cooperation Organization has taken on a broad view of cyber attacks, including the use of cyber-technology to disrupt political stability. Hence, this statement falls under the ambiguous sense.

Similar opinion was presented by Roscini in 2010. He argued that 'cyber attacks' are "a hostile use of cyber force, which could be an isolated act, the first strike of an armed conflict, an attack in the context of an already initiated armed conflict, or a reaction against a previous conventional or cyber attack"[97]. Although this concept focuses on computers and computer networks as weapons (rather than targets), neither it excludes kinetic attacks on computer facilities nor covers cyber espionage and cyber propaganda. Additionally, this framework can not explain the situation which refers to using a computer network in Nevada to operate a predator drone for a kinetic attack in Pakistan[98]. Whether it was a cyber attack or it was just a technologically advanced conventional attack? Therefore, this type of definition is not consistent with the purpose of research.

3.1.3. Recommended definition

Despite the fact that each strategy seeks to meet a distinct policy justification, none of them fully addresses the novel concerns of cyber-attacks. Currently, a modern approach has been accepted as the best of the possible definitions, and relies heavily on the Tallinn Manual. Rather than being a doctrine, the manual is an analysis of how international law applies to cyber operations in the view of 19 members of the so-called 'International Group of Experts' (IGE). In an attempt to lay out the commonly accepted norm, the Tallinn Manual's Rule 92 offers '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'[99]. As used in this Manual, cyber attack is a term of art referring to a specific category of cyber operations. Indeed, cyber attacks can be used to describe defending and attacking information and

[96] Agreement between the Governments of the Member States ShangHai Cooperation Organization on the cooperation in the field of International Information Security, 61st plenary meeting, 2008
[97] ROSCINI, Marco. World Wide Warfare – *jus ad bellum* and the Use of Cyber Force. Max Planck Yearbook of United Nation Law, 2010, Vol.14, pp.85-130
[98] HATHAWAY, Oona A. et al. The Law of Cyber - Attack. California Law Review, 2012, Vol.100, pp.817-885
[99] Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, pp.415- 420

computer network activities in cyberspace[100]. The focus on what constitutes a cyber attack is the consequence of cyber operations, or the 'consequential harm' flowing from the cyber operation[101]. Particularly, results of cyber attacks in this definition are extended to any reasonably foreseeable consequential damage, destruction, injury, or death.

To clarify the definition of Tallinn Manual, Roscini proposes an identical definition in 2012, that 'cyber attacks are those cyber operations, whether in offence or in defence, intended to alter, delete, corrupt, or deny access to computer data or software for the purposes of (a) propaganda or deception; and/or (b) partly or totally disrupting the functioning of the targeted computer, computer system or network, and related computer-operated physical infrastructure (if any); and/or (c) producing physical damage extrinsic to the computer, computer system, or network'[102]. Accordingly, cyber attacks could be utilized as stand-alone operations, or used in conjunction with a subsequent kinetic or cyber operation that they intend to enable or facilitate, or be employed in armed conflict. In all cases, a cyber 'attack' involves an action, in offence or in defence, that is carried out in or through cyberspace, but not always over a network, could target either information systems or infrastructure control systems and the result could be malfunctions or even severe harm.

The definition offered here respects both approaches taken by States and international law scholars. It added all important factors, including: mode, motivations, assets targeted and consequences of cyber attacks. It is worth emphasizing that there are no common and binding definitions for the term of cyber attack, they are understood to mean different things in different approaches. Yet, from this thesis particular point of view, the approach that Roscini has suggested can serve as an adequate framework.

3.2. The key characteristics of cyber attacks

Based on the objective definition of Roscini, the following fundamental characteristics should be outlined:

Actors or sources: The definition does not mention the author or the victim in each cyber attack, but it implicitly concerns at least two involved actors, notably the owner of the

[100] BURKADZE, Khatuna. A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace. The Fletcher Forum of World Affairs, 2020, Vol. 44, No. 1, pp.33-47.
[101] Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, pp.415- 420.
[102] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 10-18.

asset that is targeted and an adversary. The cyber operations can be launched not only by nation states, but also by non-state actors (individuals).

Objective: The targets of cyber attacks are not necessarily limited to the computer system or data themselves, it can affect computer-operated physical infrastructure and physical objects extrinsic to a computer, computer system, or network.

Motivation: The motivations for cyber attacks are propaganda or deception.

Techniques: The cyber attacks can be conducted not only through computer networks, but also through close access to the system.

Effect on targeted assets: Cyber attacks result in the alteration, deletion, corruption, deception, degradation, disablement, disruption, or destruction of assets as well as denying access to assets. The description divides the impacts of cyber-attacks into three categories: logical, physical, and cognitive. As logical effects, cyber attacks can cause denial of access. Cognitive effects include deception, meaning the use of false information to convince an adversary that something is true. Physical consequences will be caused in case of the destruction of capital.

As has been observed by another scholar, there are some features in reality that help to distinguish cyber attacks from conventional attacks, namely: indirectness, intangibility, locus factor and unpredictable effects[103].

Indirectness is is one typical characteristic of cyber attacks. It refers to a situation that a huge number of possible attacks will manipulate one system to achieve the desired result[104]. Indirect attacks, for example, include tampering with GPS satellite systems to cause enemy missiles to miss their targets or disabling air traffic control systems. It should be highlighted, however, that the causal nexus between an offensive State's act and the victim State's damaging effect will be crucial.

Intangibility is the other characteristics of cyber attack, in terms of three level: target, technique and outcome.

[103] DINNISS, Heather. Cyber Warfare and the Laws of War. Cambridge University Press, 2012, pp. 65 – 74.
[104] Id

Intangible target: On 30 April 2007, Estonian critical information infrastructure, such as Domain Name Servers (DNS), international routers, and telecommunications company network nodes, along with the largest service provider Elion, as well as the state data communication network, were targeted by coordinated and sophisticated cyber attacks[105]. The firewalls and servers of public institutions were targeted as well[106]. In July and August 2008, Georgia also reports the cyber attacks during the conflict with Russia. Targets of DDoS attacks included 54 Georgian websites, including about 90% of state institution (gov.ge) websites and a large number of .ge domain addresses[107]. As we can see from the examples, cyber attacks mainly aim at computer data, websites, information online which cannot be touched, held, sensed by the human mind, and has no physical substance. They are intangible due to their nonphysical nature.

Intangible weapon: Cyber attacks come in a number of popular cyber weapons, commonly viruses, worms, Trojans and bots[108]. They are all part of a class of software called "malware" (malicious software). Malware is known as 'code or software that is specifically designed to damage, disrupt, steal, or in general inflict some other "bad" or illegitimate action on data, hosts, or network'[109]. There are few of the most popular malware programs that were used in the certain context of cyber attacks, such as: Stuxnet, Flame, DuQu and so on. Unlike traditional weapons, the nature of malware is an artificial intelligence-based product with intelligent behaviours[110]. Malware has been noted to have many intelligent features like the ability to deceive their targeted victims and stealth capabilities to prevent detection[111]. In addition, data can also be weaponized in new ways using these attacks, depending on the way data is collected, stored, and used.

Intangible consequence: The cyber attacks do not always cause physical harm (breaking a generator) or human injury (mass causalities). By contrast, it might target the logical (e.g. disrupt a software service), the cognitive (convince or disrupt an adversary using

---

[105] POPESCU, Nicu, SCRIERRU, Stalislav (eds). Hacks, leaks and disruptions: Russian Cyber Strategies. European Union Institute for Security Studies, 2018, pp.52-58.
[106] Id
[107] Id, pp.59-60.
[108] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129.
[109] What Is the Difference: Viruses, Worms, Trojans, and Bots?. Cisco Security. Available at https://tools.cisco.com/security/center/resources/virus_differences
[110] JONATHAN, Pan Juin Yang, FUNG, Chun Che. Artificial Intelligence in Malware - Cop or Culprit?. Murdoch University, pp.181-184.
[111] Id

false information), as well as in the case of an attack on a New York stock exchange[112]. It has the potential to produce chaos and panic in the US stock market.

Locus factor: In the context of force, a kinetic attack can almost always be easily traced to a geographical source[113]. The fact that it is very challenging to verify the territorial point of cyber attack's origin, especially when such attacks may be sourced worldwide rather than just from a few locations. By way of illustration, there were more than one million computers involved from 178 countries altogether (mainly sourced outside of Estonia) during the attack on Estonia in 2007[114]. As a result, spoofing allows an attacker to conceal his location and makes it harder for others to pinpoint the source of a cyber attack. In others, the wrong identity of the attackers convinces the victim that the attack originated elsewhere.

Unpredictable effects: The results of cyber attacks are highly unpredictable unlike those of kinetic attacks because cyber attacks can happen anytime, anywhere, particularly when they are carried out by sophisticated weapons. As history has shown, from the Stuxnet worm to Flame or Duqu, when malware is fast and designed to propagate, the possible results span the spectrum from mere inconvenience to catastrophic damage. Even though the Stuxnet virus in reality caused some delays and disruptions in the uranium enrichment process, experts believe that the Stuxnet may result in a serious disaster if the plant becomes operational[115]. It is because with control systems disabled by the virus, the reactor would have the force of a "small nuclear bomb". Thus the attacks could easily spill over into geopolitical tensions rather than internal issues. Furthermore, we now live in a digital world that is so interconnected that a single server attack can have global consequences. For example, in 2003, the so-called Sapphire worm not only took down serves in South Korea, but also disrupted internet services in Thailand, Japan, Malaysia, Philippines and India[116]. Likewise, the years 2008 and 2009 witnessed the Conficker Worm infecting an estimated five million

---

[112] DINNISS, Heather. Cyber Warfare and the Laws of War. Cambridge University Press, 2012, pp. 65 -74.
[113] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129.
[114] TIKK, Eneken et al. International Cyber Incidents: Legal consideration. Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010, pp. 14-33.
[115] JAHN, George. Stuxnet virus penetrates nuclear plant, may cause Chernobyl-like disaster. Available at https://www.csmonitor.com/World/Latest-News-Wires/2011/0131/Stuxnet-virus-penetrates-nuclear-plant-may-cause-Chernobyl-like-disaster
[116] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129

personal computers in over two hundred countries[117]. As such, the effects of cyber attacks are becoming increasingly difficult to predict and control.

One of the features of this new kind of attack that should be discussed here is the method of conducting a cyber attack. In practice, the most commonly known methods to launch a cyber attack are the corruption of hardware or software, or flooding the system with so much information to cause its collapse[118].

The first mean (corruption of hardware) is carried out by Trojan horses, logic bombs, viruses, and worms, which can be installed in a computer through chipping, hacking, via a portable storage device, or by inadvertently downloading them from a website or an email attachment[119]. A virus can replicate itself to a legitimate program on the target computer, modify it and subsequently infect other programs and, if the computer is connected to a network, potentially other computers as well[120]. As contrasted with a virus, a worm is an independent program that can copy itself onto other computers but usually does not modify other programs. Worms can 'cause damage merely by eating up network resources or destroying data and are particularly effective over networks'[121]. Especially, worms do not require activation or any human intervention to execute or spread their code[122]. Trojan Horses are code fragments that conceal worms or viruses and allow remote access to systems by attackers[123].

Another type of attack is known as Distributed Denial of Service (DDoS) attacks, which have been the most prevalent form of cyber attack in recent years. This method of attack was demonstrated in Estonia in 2007 and Georgia in 2008. This method can be used to take down major information networks by flooding an Internet site, server, or router with data requests to overwhelm its capacity to function [124]. In these attacks, coordinated botnets (short

---

[117] Id
[118] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.18.
[119] Id, p.18.
[120] COX, Stephen J. Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War. Houston Law Review 42, 2005, pp.888 -889.
[121] BARKHAM, Jason. Information Warfare and International Law on the Use of Force. Interntional Law and Politics, 2002, Vol.34, p.63.
[122] DINNISS, Heather H. Cyber Warfare and the Laws of War (Cambridge Studies in International and Comparative Law). Cambridge University Press, 2012, p.259.
[123] BARKHAM, Jason. Information Warfare and International Law on the Use of Force. Interntional Law and Politics, 2002, Vol.34, p.63.
[124] WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). The Yale Journal of International Law, 2011, Vol.36, p.423.

for 'robot networks') play an important role because they are the source of most spam, networks of infected computers hijacked from their unaware owners by external users[125].

3.3. Classification

Different classifications of cyber attacks have been introduced by the US National Military Strategy for Cyberspace Operations, including computer network attacks (CNA), computer network defense (CND), and 'related computer network exploitation enabling operations' (CNE).

3.3.1. Cyber Network Attacks (CNAs)

The US National Military Strategy for Cyberspace Operations describes CNAs as 'operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves'[126]. The NATO Glossary of Terms and Definitions coined a similar explanation for CNA, but it distinguishes between those that target the computer or computer network and those that target the information contained in the computer or computer network[127]. Likewise, CNA is mentioned in the HPCR Manual as an operation that 'manipulates' computer information and that aims 'to gain control over the computer or computer network'[128].

The preceding definitions mainly focus on computers and computer systems as targets and do not specify how the attack must be carried out (cyber, electronic, or kinetic).
Differently, CNAs are more precisely defined in the Joint Terminology for Cyberspace Operations as 'actions […] taken through the use of computer networks to disrupt, deny, degrade, manipulate, or destroy information resident in the target information system or computer networks, or the systems/networks themselves'[129]. According to this definition, the term 'cyber attack' has broader scope than CNA because cyber attacks can be conducted through computer networks or through close access to the system. The effects of cyber attacks are also much more widespread because they are not restricted to the intended computer system or data.

---

[125] BAKER, Stewart Baker, WATERMAN, Shaun Waterman, et al. In the Crossfire—Critical Infrastructure in the Age of Cyber War, 2009, p. 6. Available at http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf
[126] US National Military Strategy for Cyberspace Operations, p GL–1.
[127] NATO's Glossary of Terms and Definitions, p 2–C–11.
[128] Rule 1(m), HPCR Manual, p 20
[129] Joint Terminology for Cyberspace Operations, p 3

3.3.2. Cyber Network Defence (CND)

CND is the term that the US National Military Strategy for Cyberspace Operations coins a distinguished definition to CNA. Meanwhile, the NATO Glossary of Terms only distinguishes between CNAs and CNEs, leaving a blank space for CND. According to the US National Military Strategy for Cyberspace Operations, CND are 'actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks'[130]. CND comprises both active and passive cyber defenses, as well as information assurance, intelligence, counterintelligence, law enforcement, and military capabilities[131].

3.3.3 Cyber Network Exploitation (CNE)

Cyber attacks must be distinguished from cyber exploitation**.** Firstly, cyber exploitation aims to gain illegal access to computers, computer systems, or networks in order to steal data, whereas cyber attacks aim to disrupt the operation of the accessed system or change or delete the data stored there[132]. Secondly, cyber attacks and cyber exploitation have different techniques. The former uses destructive payload to execute whilst the latter acquires information – nondestructively[133]. Last but not least, cyber exploitation activities are distinct in that they have no impact on the system's functionality. They are more concerned with intelligence gathering, surveillance, and reconnaissance than with system disruption, and they can serve as a precursor to a kinetic or a cyber attack by mapping the architecture of the network or operating system to be attacked or identifying previously unknown vulnerabilities[134].

Given these issues, cyber attacks present challenges about the ambiguities of international norms, which were historically adopted to define rules related to traditional military operations. Currently, there are no direct international legal regulations for understanding the concept of cyber operations, except the non-binding source Tallinn Manual 2.0, international legal framework for triggering self-defence must be analyzed to clarify the legality of cyber operations in the digital era.

---

[130] US National Military Strategy for Cyberspace Operations, p GL–1.
[131] Id
[132] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 10-18.
[133] Id
[134] Id

CHAPTER 4

CAN CYBER ATTACKS TRIGGER THE RIGHT TO SELF-DEFENCE UNDER ARTICLE 51 OF THE UN CHARTER?

The question of how international law, specifically the provision of self-defense in the UN Charter, applies to cyber attacks is one of the most pressing today, as the threats posed by cyber attacks are growing. Due to the establishment of new operational domains and the use of cyber technological advances by attacking states, the following questions should be asked: 'Can states have the right to use individual or collective defense against a cyber attack?'. Having in mind that the debate over cyber attack remains active. Specifically, Articles 2(4) and 51 of the United Nations ("UN") Charter governing the prohibition on the use of force and right to self-defence are at the heart of the debate. This chapter will examine the challenges of fitting cyber-attacks into existing legal categories 'use of force' and 'armed attack', then elaborate the important question of whether and when a cyber attack constitutes an armed attack according to Article 51 UN Charter and hence allows a state to invoke the right to self-defence. It is significant to consider that in order for a cyber attack to amount to an armed attack, it has to be considered use of force first[135].

4.1. Do cyber attacks constitute a "use of force"?

In the absence of what constitutes the use of force, the question raises of whether or not cyber attacks fall within the ambit of Article 2(4) UN Charter. The difficulty is cyber operations did not exist when the UN Charter was adopted in 1945. Neither Article 2(4) nor its customary is remedial in nature[136], according to Professor Schmitt. Recent scholarly writing has produced at least four prominent theories concerning the issue of cyber attacks and the threshold of force, including: instrument-based, target-based, effects-based and the CPS (cyber physical system) – focused approach.

[135] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 44-69
[136] SCHMITT, Michael N. Cyber Operations and The *Jus Ad Bellum* revisited. Villanova Law Review, 2011, pp. 569-605.

4.1.1. Leading approaches

The classic instrument-based method generally focuses on the use of traditional military weapons. In other words, the means to carry out an act is seen as a decisive factor. However, such approach was not supported by the ICJ cause in Advisory Opinion of July 1996 the Court concluded that Article 2(4) 'does not refer to specific weapons but applies to any use of force, regardless of the weapon employed'[137] and the Charter 'neither expressly prohibits, nor permits the use of any specific weapon, including nuclear weapon'[138]. Under this approach, cyber attacks do not qualify as use of force in Article 2(4) even when they result in physical damage because they 'lack the physical characteristics traditionally associated with military coercion'[139]. Given the fact that cyber-attacks can potentially cause catastrophic destruction without using traditional military weapons[140], the majority of academics have rejected this outdated model. As Professor Schmitt claims, such an approach 'eases the evaluative process by simply asking whether force has been used, rather than requiring a far more difficult assessment of the consequences that have resulted.'[141]

The target-based approach suggests attacks against critical national infrastructure from any source constitute a use of force[142]. It means cyber attacks may rise to the level of an unlawful use of force when they are conducted against 'national critical infrastructure' system, even in absence of significant destruction or causalities[143]. However, this approach also has been criticized since it might suffer from over-inclusion. Indeed, its broad scope would include cyber operations that solely intend to cause inconvenience or collect information of national critical infrastructure[144]. In other words, merely stealing or compromising sensitive military information could also qualify as an use of force even though no immediate loss of life or destruction results[145]. As a result, a cyber-attack on a crucial

---

[137] Advisory Opinion of The International Court of Justice of 8 July 1996, Legality of the Threat or Use of Nuclear Weapons, paragraph 39.
[138] Id
[139] HOLLIS, Duncan B. Why the State need an Inetrnational Law for Information Operations. Lewis and Clark Law Review, 2007, Vol.11, pp.1024-1057.
[140] HATHAWAY, Oona A. et al. The Law of Cyber - Attack. California Law Review, 2012, Vol.100, pp.817-885
[141] SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 1999, pp. 914.
[142] JENSEN, Eric Talbot. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Brigham Young University Law School, 2002, pp. 221.
[143] HOLLIS, Duncan B. Why the State need an Inetrnational Law for Information Operations. Lewis and Clark Law Review, 2007, Vol.11, pp.1024-1057.
[144] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 44-69
[145] JOYNER, Christopher C., LOTRIONTE, Catherine. Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 2001, Vol.12, No.5, pp. 825-865.

national system is enough to justify a conventional military reaction that could lead to an armed conflict. If this doctrine is broadly accepted, the chances of cyber-wars evolving into catastrophic conventional armed conflicts would rise. In addition, this model is not reasonable because there is no general definition of what constitutes a 'critical infrastructure and vital interests' of a country[146].

The third method is the so-called effects - based approach or the consequentiality approach. This method is primarily based on the gravity of damage caused and not on the means of attack used. Therefore, any cyber operation that cause or are reasonably likely to cause the same effects of kinetic weapons would equally be considered a use of force. This approach is favored by the United States. The US National Research Council agreed that 'the legal status of any military activity is judged by its effects (regardless of the means) according to the criteria of the UN Charter and *jus ad bellum*'[147]. Therefore, cyber attacks 'should be judged primarily by the effects of an action rather than its modality'[148] and if the effects to be produced by a cyber attack would have the same effects as certain kinetic and other means that are generally treated as the use of force. Similarly, Professor Schmitt admitted that cyber operations that 'directly result (or are likely to result) in physical harm to individuals or tangible objects equate to armed force, and are therefore uses of force'[149].

In a similar spirit, the Tallinn Manual 2.0 produced a set of assessment criteria to determine if cyber attacks are a form of force. These criteria are severity, immediacy, directness, invasiveness measurability of effects, military character, state involvement and presumptive legality. They are based on a set of seven non-exhaustive factors that Professor Schmitt recommended in his earlier article in 1999[150]. These factors represent the main differences between permissible (economic and political) and impermissible (armed) instruments of coercion. Nevertheless, they are not binding and not formal legal criteria. The factors are as follows:

---

[146] VALUCH, Jozef; HAMUĽÁK, Ondrej. Use of Force in Cyberspace. International and Comparative Law Review, 2020, vol. 20, no. 2, pp. 174–191.
[147] US National Research Council. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. National Academy Press, 2009, pp.33-34
[148] Id
[149] SCHMITT, Michael N. Cyber Operations and The Jus Ad Bellum revisited. Villanova Law Review, 2011, pp. 569-605.
[150] SCHMITT, Michael N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. Columbia Journal of Transnational Law, 1999, pp. 885–937.

1) Severity: This is the most significant factor in the analysis. It basically is about the type and scale of the harm. According to this component, any act that causes physical harm to people or property amounts to the use of force. This does not apply to those generating only minor inconvenience or irritation. In this context, the level, extent and duration of the consequences will have a major impact on the assessment of the seriousness of cyber operations.

2) Immediacy: This factor focuses how quickly the harm materializes after the attack. Actions that have immediate negative outcomes and do not allow enough time to minimize the harm are more likely to be perceived as using force rather than those that are delayed or appear slowly and continuously.

3) Directness: This factor examines the causal link between the cyber operation and the consequences. It is based on the argument that the consequences of armed coercion are directly linked to *actus reu.* In armed actions, cause and eventual effect are closely related. An explosion that directly damages people or objects is an example of this.

4) Invasiveness: It refers to the degree to which the attack penetrates the victim state's territory. It may be stated that the greater interference with the victim state's sovereignty and territory, the more likely it is to be considered use of force. By way of illustration, economic coercion may involve no intrusion at all (trade with the target state is simply cut off), whereas in the case of armed coercion forces from one state always infringe on the sovereignty of another. The former does not qualify as a use of force, whereas the later does.

5) Measurability: This element mentions the degree to which the harm can be quantified. While the harm caused by armed attack is generally measurable, the negative impact of other forms of coercion on the other hand is difficult to quantify. It may be true in the cyber attack realm when the consequences are less apparent. As a result, a cyber operation that can be evaluated precisely (e.g., amount of data corrupted, percentage of servers disabled, number of confidential files exfiltrated) is more likely to be classified as a use of force than one with difficulties to measure impacts.

6) Presumptive legitimacy: As a rule in international law, acts which are not forbidden are permitted. Thus, in the absence of an express restriction, an act is presumed to be legal. For instance, it is well accepted that international law does not prohibit propaganda,

psychological operations, espionage, or mere economic pressure. To the degree that such activities are carried out through cyber operations, they are presumptively legal unless there exists a ban related to them.

7) Responsibility or State involvement: This element concerns the scenarios in which a state will be held liable for a cyber operation performed by that state itself. The closer and clearer the nexus between the cyber operation and a state, the more likely it will be characterized as a use of force.

8) Military character: This is a new criterion introduced in Tallinn Manual 2.0, but it was not suggested by Professor Schmitt. It has been argued that the simple link between a cyber operation and a military operation enhances the possibility that it will be labeled as a use of force. This argument is likely supported by the UN Charter. Indeed, its preamble provides that 'armed force shall not be used, save in the common interest', whereas Article 44 in turn, uses the term "force" without the qualification "armed" in a situation which clearly refers to the use of military force[151]. Further, the use of force has traditionally been understood as the force using military or other armed forces.

The newest framework was developed by Reese Nguyen, that is 'administrable across nation states, forward-looking, and both consistent and sensible in its treatment of cyber attacks'[152]. Nguyen suggests a method which crystallizes some core values of the target-based approach and the effect-based approach. Accordingly, cyber attacks only constitute an armed attack if 'they are intended to cause irreversible disruption cyber-physical'[153]. It encompasses physical damage and the cyber-physical system component as the consequence and object of the attack respectively. However, the central part of this approach focuses on the intention of an attack, because a cyber attack aimed at a computer system without a physical control could rise to the level of armed attack 'if it is intended to cause or may foreseeably cause irreversible disruption or damage'[154]. Nguyen's approach is one of good attempts at developing an applicable framework for analyzing cyber-attacks, but suffers from theoretical and practical shortcomings. The first concern is how we could prove the intention of cyber

[151] Article 44 of the UN Charter: "*When the Security Council has decided to use force it shall, before calling upon a Member not represented on it to provide armed forces in fulfilment of the obligations assumed under Article 43, invite that Member, if the Member so desires, to participate in the decisions of the Security Council concerning the employment of contingents of that Member's armed forces*."
[152] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 ,p.1125
[153] Id
[154] Id,

attacks to cause damage in order to warrant self-defence, especially when it is merely in preparation. Assuming that we can ascertain the intentional damage in the event a firewall detected and prevented a cyber-attack or a virus that nevertheless caused damage on purpose, under this framework the target state would be permitted to use self-defence in retaliation[155]. Additionally, Nguyen's model covers all attacks that are 'intended' to cause physical damage, meaning that an attack need not occur yet still activate the right to self-defence. In this regard, the logic of the CPS (cyber physical system) - focused approach may satisfy both the preemptive and preventive self-defense doctrines, thus it is not compatible with the wording of Article 51 of the UN Charter.

4.1.2. The most prominent approach

It must be noted here that although all leading approaches provide useful analogies in an attempt to confront cyber attacks, none of them has escaped criticism[156]. From the practical point of view, each one falls short of adequately addressing the novel problems of cyber-attacks[157]. Nevertheless, there are several arguments in support of the effects-based approach.

The effects-based approach is supported by the jurisprudence of International Court of Justice. In the Nuclear Weapons advisory opinion, the Court concluded that the *jus ad bellum* applies to 'any use of force, regardless of the weapons employed'[158], suggesting that the instrument-based approach is not best suited in assessing whether a cyber attack amounts to the use of force. Recall that the Court in Nicaragua case specifically considered the certain 'scale and effects' of the attack to resolve whether an attack meets the armed attack threshold. The findings of the Nicaragua case and Nuclear Weapons case illustrate that cyber-attacks can amount to an armed attack heavily depending on the 'scale and effects' of the attack, regardless of the means. Apparently, effects-based jurisdiction requires such an effect and its gravity to be sufficient to reach the level of an armed attack. Following this criteria of ICJ, the model of effect-based approach is fundamentally based on the gravity of consequences or effects of a cyber activity.

---

[155] SIMMONS, Noah. A Brave New World Applying International Law of War to Cyber-Attacks. Journal of Law & Cyber Warfare, 2014, Vol. 4, No. 1, p.66-67.
[156] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , pp. 1079-1129.
[157] SIMMONS, Noah. A Brave New World Applying International Law of War to Cyber-Attacks. Journal of Law & Cyber Warfare, 2014, Vol. 4, No. 1, p.53.
[158] Advisory Opinion of The International Court of Justice of 8 July 1996, Legality of the Threat or Use of Nuclear Weapons, paragraph 39.

However, simply focusing on the outcome is not consistent with traditional notion in Article 2(4) UN Charter, because the language of UN Charter provision covers merely "armed" force and disallows political or economic pressure. Historically, the drafters of the UN Charter and the Declaration of Friendly Relations explicitly rejected a proposal to further encompass economic coercion as a use of force[159]. The model of consequence-based approach, in particular Schmitt's formula, consists of seven factors that highlights the key difference between legal (economic and political) and illegal (armed) instruments of coercion, thus it is in keeping with the Article 2(4). Resultantly, a cyber operation that involves such economic or political coercion is definitely not a prohibited use of force. This method seems to be in accordance with the widely accepted interpretation of Article 2(4) UN Charter to the extent that if the physical consequences of a cyber attack inflict comparable physical damage to activating a bomb or launching a missile, that cyber attack should be considered a use of force.

There are two cases of cyber attacks in practice that help evaluate Schmitt's framework: the case of Estonia in 2007 and the case of Iran in 2010. The Estonian cyber-attack began on April 27, 2007 with widespread cyber attack on Estonian websites, including those of the Estonian government, the parliament, banks and newspapers. The cyber attackers employed several methods including Denial of Service (DoS) attacks, Distributed Denial of Service (DDoS) attacks, website defacement, attacks against Data Name Servers (DNS), and mass email comment spam. The most serious attacks were launched on 9-15 May against state institutions, telecommunications companies, and the country's two largest banks (Hansapank and SEB Eesti Ühispank). Although the Estonian governmental institutions were the primary victims of the attack, Hansapank, the largest Estonian bank, was also affected by the DDoS attacks. The cyber-attacks had a noticeable effect on the Estonian economy, affecting commerce, industry, and governance that relied on information and communications technology (ICT) infrastructure[160]. Besides, legitimate Internet traffic was blocked[161].
Even though Estonia accused Russia's Government, Moscow denied involvement in the 2007 cyber-attacks in Estonia.

---

[159] AZUBUIKE, Eustace Chikere. Probing the Scope of Self Defense in International Law. Annual Survey of International & Comparative Law, 2011, Vol. 17, Issue 1, Article 8, p.140.
[160] STEPHEN, Herzog. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 2011, pp. 49-60.
[161] TAMKIN, Emily. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for CyberThreats?. Available at https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/

Severity: The cyber attacks caused no loss of life or injury to person, or substantial property damage. The attacks fundamentally affected the financial and social security system of Estonia. However, the lack of internet access for the largest banks led to an economic loss because this country is more dependent on online-based communication and trade. Although the consequences went beyond mere inconvenience or irritation, they were not critical. *Directness:* These attacks were direct, as with the inability to access funds and interference with the distribution of government benefits. *Immediacy:* The effects were not only immediate, but also wide-spread and long term. *Invasiveness:* some of the targeted systems were designed to be very secure, therefore the operations were highly invasive. *Measurability:* Most attacks involved denial of service, rather than destruction of data, thus the outcomes were very difficult to estimate. *Presumptive legitimacy:* In terms of force, political and economic actions are presumed to be legitimate. These operations were more than merely pressuring the target state because they involved intentionally frustrating governmental and economic functions (the websites of the Estonian Parliament, President and Prime Minister). Since Estonia is a highly digitised country and heavily reliant on technology, this implies that these attacks on central figures in Estonian politics are a clear violation of political independence, thus amount to 'use of force'. *State involvement:* Regarding the attribution of responsibility for the cyber attacks, foreign cyber security experts who investigated the 2007 events in Estonia agreed that they were carried out by voluntary or 'patriotic' non-state hackers who sympathised with the Russian government's views[162]. However, the nexus between the action and the State was ambiguous. *Military character:* There was no military character in this circumstance. Taking into account all of the criteria, it is not convincing to conclude that the incident reaches the threshold of the use of force.

The second case happened in Iran in 2010. Natanz is known as a nuclear plant that was used to enrich uranium. It also was the target of malware, the so-called "Stuxnet worm". The Stuxnet worm was designed to aim at Iran's Natanz uranium enrichment facility. Specifically, the worm exploited the software used in programmable logic controllers (PLCs) used to automate machine processes [163]. These PLCs controlled frequency converter drives, which in turn controlled the centrifuge speeds. Stuxnet reportedly destroyed 1,000 centrifuges by

[162] EVRON, Gadi. Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War. Georgetown Journal of International Affairs, 2008, no. 1, pp. 122–123.
[163] FOLTZ, Andrew, C. Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate. Joint Force Quarterly, 2012, issue 64, p. 44.

manipulating the speed of already temperamental and frequency-sensitive centrifuges over time (weeks and possibly months)[164].

Severity: In this case, Stuxnet produced material damage to physical property or physical destruction to centrifuges. More importantly, the damage was significant because it harmed a vital Iranian interest, namely the country's nuclear program. *Immediacy*: Concerning this incident, there were three periods of attack in over ten months[165]. The damage took weeks or even months to manifest. Generally, the immediate factor cannot be assessed in this case because it did not satisfy. *Directness*: Stuxnet appears to have a direct causal relationship with the damaged centrifuges. Stuxnet was designed to force a change in the centrifuge's rotor speed at the Natanz uranium enrichment plant, inducing excessive vibrations or distortions that would damage the centrifuges[166]. *Invasiveness*: Stuxnet appears to have targeted Iran's sensitive and highly secure national systems as well as crossing international borders. It means Stuxnet represents a significant intrusion on Iranian sovereignty[167]. *Measurability*: The consequences are completely quantifiable, based on Iran's already high centrifuge failure rate. *Presumptive legitimacy*: There is no provision in international treaties or customary law that authorizes the use of force to harm a country's nuclear facilities. As a result, Stuxnet does not enjoy presumptive legitimacy. *Responsibility*: Despite the fact that no government has claimed responsibility for Stuxnet, the worm's purpose and design strongly suggest government involvement. It is also possible that Stuxnet was created and launched by nonstate actors. The Schmitt analysis suggests that most states would regard Stuxnet as a use of force. The worm was extremely invasive, caused direct and measurable physical damage, certainly lacks a clear presumption of legitimacy, and probably involved state support. Indeed, the formula treats cyber attacks that cause or are reasonably likely to cause material damage to property or persons equitably to kinetic attacks. On the other hands, a cyber operation which causes minimal damage such as the destruction of a single computer or server would clearly not fall within the scope of the provision of Article 2(4)[168].

---

[164] Id
[165] FOLTZ, Andrew, C. Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate. Joint Force Quarterly, 2012, issue 64, p. 45
[166] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 44-69.
[167] Id
[168] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p. 54.

Once the cyber attack crosses the threshold of a 'use of force', the extent of the attack can be measured to determine whether there has been an armed attack, which would trigger the right to self-defence in Article 51[169]. It is true that Article 51 of the UN Charter was drafted consistent with the instrument-based approach. However it does not mean the choice to use an instrument-based approach is sufficient to address self-defense claims against cyber attacks. This is because armed attacks by definition involve kinetic military force, whereas cyber attacks frequently employ non-kinetic approaches. The instrument-based approach falls short of explaining cyber attacks that do not sufficiently resemble armed attacks but have the same overall impact[170]. In such a context, the effect-based approach makes more sense.

The idea that the result-based framework does not cover the situation of attacks with delayed effects[171] or unsuccessful effects[172]. It is worth noting again that under consequence-based approach, armed attack must also be understood in scope of the effects typically linked with the term 'armed'[173]. The nature of an armed operation is the death or injury of people, as well as the damage or destruction of property and other tangible objects. An armed attack may not be carried out by conventional military force, but its effects must be comparable to those of such weapons. If we rely on intentional damages logic, the cyber attacks with unsuccessful effects or delayed effected should be qualified as use of force and also an armed attack as long as the intent of the attack exists. However, this interpretation may seem completely unsatisfactory in the context of the massive and grave consequences that cyber operations can cross the threshold of 'use of force' even when no physical harm is done to people or property or these attacks demonstrate no severe effects. More importantly, the majority of commentators agree on the difficulty of determining the intent of a cyber attack[174]. In that way, the CPS-focused approach is overbroad in its scope.

As mentioned in Tallinn 2.0 and claimed by Roscini, Schmitt's criteria are 'not legal' and 'merely factors that can be expected to influence States when making use of force

---

[169] BARKHAM, Jason. Information Warfare and International Law on the Use of Force. Interntional Law and Politics, 2002, Vol.34, p.85.
[170] BURKADZE, Khatuna. A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace. The Fletcher Forum of World Affairs, 2020, Vol. 44, No. 1, p.43.
[171] BARKHAM, Jason. Information Warfare and International Law on the Use of Force. Interntional Law and Politics, 2002, Vol.34, p.87.
[172] NGUYEN, Reese. Navigating "Jus Ad Bellum" in the Age of Cyber Warfare. California Law Review , 2013, Vol. 101, No. 4 , p. 1122.
[173] SCHMITT, Michael N. Cyber Operations and the *jus ad bellum* Revisited. Villanova Law Review, 2011, p.588.
[174] SIMMONS, Noah. A Brave New World Applying International Law of War to Cyber-Attacks. Journal of Law & Cyber Warfare, 2014, Vol. 4, No. 1, p.83.

appraisals'[175]. Furthermore, these factors must be considered in conjunction when determining whether such operations can reach the use of force threshold[176]. For example, highly invasive operations that cause only inconvenience (e.g. DoS operations – temporary denial of provision of services) are unlikely to be classified as the use of force[177]. On the other hand, massive cyber operations that severely damage the economy may be categorized as the use of force despite the fact that economic pressure is not prohibited in international law. Although these criteria have stood the test of time, they should be used in a specific context, and the importance of different factors and how they should be weighted will vary from case to case. In general, both Schmitt's formula and Tallinn's guiding criteria provide the useful method to distinguish armed force from other forms of coercion. Accordingly, armed force results in more significant physical injury or destruction of property, with greater immediacy and in a more direct way.

As such, to examine whether cyber attacks can reach the threshold of use of force by applying Schmitt's analysis or Tallinn's criteria, the effects of cyber attacks are worthy to note. As discussed in Chapter 2, cyber attacks can produce unpredictable and multiple effects. According to Roscini, cyber attacks consist of primary effects, secondary effects, and tertiary effects. The primary effects are those on the attacked computer, computer system or network, i.e. the deletion, corruption, or alteration of data or software, or system disruption through a DDoS attack or other cyber attacks[178]. The secondary effects are those on the infrastructure operated by the attacked system or network (if any), i.e. its partial or total destruction or incapacitation[179]. Tertiary effects are those on the persons affected by the destruction or incapacitation of the attacked system or infrastructure, for instance those that benefit from the electricity produced by a power plant incapacitated by a cyber operation[180].

In the modern context, the secondary effect of cyber attacks may raise the question of whether cyber attacks severely disrupting critical infrastructure also fall under the scope of Article 2(4) if the disruption caused is significant enough to affect state security. Regardless this issue, the critical character of the targeted infrastructure plays an important role in

[175] Rule 69, Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, pp.333.
[176] VALUCH, Jozef; HAMUĽÁK, Ondrej. Use of Force in Cyberspace. International and Comparative Law Review, 2020, vol. 20, no. 2, pp. 174–191.
[177] Id
[178] ROSCINI, Cyber Operation and Use of Force. Oxford University Press, 2014, pp. 44-69.
[179] Id
[180] Id

determining when a disruptive cyber operation amounts to a use of force under Article 2(4). As we mentioned above, the definition of what is 'critical infrastructure' heavily relies on the policy considerations of states. Currently, different states have different definitions of what constitutes 'critical infrastructure'[181]. For instance, in the Commission of the European Union's view, critical infrastructures include 'those physical resources, services, and information technology facilities, networks and infrastructure assets which, if disrupted or destroyed, would have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments.'[182]. Russia, on the other hand, defines 'vital structures' as 'State's facilities, systems and institutions, deliberate influence on the information resources of which may have consequences that directly affect national security (transport, energy supply, credit and finance, communications, State administrative bodies, the defence system, law-enforcement agencies, strategic information resources, scientific establishments and scientific and technological developments, installations that pose heightened technological and environmental risks, and bodies for eliminating the consequences of natural disasters or other emergency situations)'[183]. Additionally, if actions that significantly interfere with the functionality of critical infrastructure (such as the banking and finance, government, and communications sectors) can reasonably be regarded as uses of force, even when no physical consequences arise, then Article 2(4) is supposed to be flexible in its interpretation in order to incorporate new uses of force. In the present, the ban of force in Article 2(4) does not cover economic or political coercion and Article 44 supports such a view as well.

4.2.Do cyber attacks constitute an 'armed attack'?

In previous parts, we found out that a cyber attack can reach the threshold of use of force if it causes loss of life, injury or destruction. Still, it is not sufficient for a victim State to justify self-defence. As mentioned in Chapter 1, under Article 51 of the UN Charter, the state will be entitled to react forcibly in self-defence only if there is existence of an armed attack (the most grave forms of the use of force). Thus the answer of whether a state can invoke the right to self-defence in case it is targeted by cyber attacks will not fall outside the scope of the above requirement. Basically, an armed attack will always be a use of force, but not every use

[181] Id, p.58.
[182] EU Commission, Green Paper on a European Programme on Critical Infrastructure Protection, COM(2005) 576 final, 17 November 2005, p 20.
Available at https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF
[183] UN Doc A/54/213, 10 August 1999, p. 10

of force is an armed attack. A victim state can only invoke the right to self-defence when being cyber attacked if these attacks rise to illegal use of force and armed attack.

To determine if a cyber attack has risen to the level of an armed attack, the method of comparison between the nature of a cyber attack and the characteristics of kinetic armed attack will be used in this section.

4.2.1. Required degree of gravity

The armed attack threshold does not only apply to operations using traditional means, but also to operations using different means. In the Nuclear Weapons case, the ICJ was of the view that Article 51 'does not refer to specific weapons' and it 'applies to any use of force, regardless of the weapons employed'[184]. By saying this, the Court confirms the view that the choice of means or weapons is irrelevant to the issue of whether an operation qualifies as an armed attack. Thus the absence of kinetic weapons in cyber attacks does not imply that they are not 'armed'. Similarly, Karl seemed to agree and persuasively presented his arguments in the book "Armed Attack":

> *It is neither the designation of a device, nor its normal use, which make it a weapon, but the intent which it is used and the effect. The use of any device or number of devices, which results in a considerable loss of life and/or extensive destruction of property must therefore de deemed to fulfill the conditions of an "armed attack"*[185]

In fact, it is universally accepted that chemical, biological, and radiological attacks of the requisite scale and effects to constitute armed attacks trigger the right of self-defence[186]. Hence, it appears plausible to assume that the deployment of cyber weapons in an attack has no effect on the applicability of the traditional 'armed attack' criterion because the consequences will play decisive role. As such, the critical deciding factor will be the effects of a cyber-attacks and whether these effects were similar to those that would result from an action otherwise qualifying as a kinetic armed attack. The effects-based approach finds broad support amongst commentators, the International Court of Justice, and the Tallinn Manual's

---

[184] Advisory Opinion of The International Court of Justice of 8 July 1996, Legality of the Threat or Use of Nuclear Weapons, paragraph 39

[185] ZEMANEK, Karl. Armed Attack. Max Planck Encyclopedia of Public International Law, 2010, paragraph.21.

[186] Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 71, pp.339-348.

International Group of Experts on the ground that the purpose of self-defense is to defend against harm itself rather than against the particular means of harm.

As presented in Chapter 1, the ICJ in the Nicaragua case back in 1986 established the 'scale and effects' approach or in other words the intensity of the effects of an attack. In that case, the Court identified scale and effects as the criteria that distinguish actions qualifying as an armed attack from those that do not. Yet, the parameters of the scale and effects criteria remain unsettled beyond the indication that they need to be grave[187].

Relevant to this issue, Dinstein suggested that the gap between 'use of force' and 'armed attack' was overemphasized by the ICJ in the Nicaragua judgment of 1986 and is in reality very narrow[188]. Further, Dinstein argued that what the gap denotes is that a use of force not involving loss of life or significant destruction of property (for instance soldiers shooting across a border killing animals) falls short of an armed attack[189]. More concretely, he also made clear in his other article that 'whenever a lethal result to human beings or serious destruction to property is engendered by an illegal use of force by State A against State B, that use of force will qualify as an armed attack'[190]. As such, once the use of force reaches the threshold of sufficient gravity, an armed attack is in progress even if it is characterized by minor magnitude[191].

On the ground of Dinstein's approach, the cyber attacks that reach the necessary destructive effects are serious enough to amount to armed attacks. It means any cyber attack that injures or kills persons or damages or destroys property would satisfy the armed attack requirement. This approach seems consistent with the definition of an armed attack in the non-cyber context[192], which argues that 'the essence of an armed operation is the causation, or risk thereof, of death of or injury to persons or damage to or destruction of property and other tangible objects'[193]. Furthermore, the ICJ held in the Oil Platforms case that it did not exclude

---

[187] Id
[188] DINSTEIN, Yoram. Cyber War and International Law: Concluding Remarks at the 2012 Naval War College nternational Law Conference. International Law Studies, US. Naval War College, 2013, Vol.89, pp.278-279.
[189] DINSTEIN, Yoram. Cyber War and International Law: Concluding Remarks at the 2012 Naval War College nternational Law Conference. International Law Studies, US. Naval War College, 2013, Vol.89, pp.278-279.
[190] DINSTEIN, Yoram. Computer Network Attack and Self-Defene. International Law Studies, US. Naval War College, 2002, Vol.76, p.100.
[191] Id, p.100.
[192] HAYWARD, Ryan J. Evaluating the 'imminience' of a cyber attack for purposes of aticipatory self-defence. Columbia Law Review, 2017, Vol.117, p.407.
[193] SCHMITT, Michael N. Cyber Operations and the *jus ad bellum* Revisited. Villanova Law Review, 2011, p.588.

'the possibility that the mining of a single military vessel might be sufficient to bring into play the inherent right of self-defense'[194]. Thus, in identifying those actions likely to be characterized as an armed attack qualitative indicators of attack (death, injury, damage, or destruction) are more reliable than quantitative ones (number of deaths or extent of destruction)[195]. As such, as long as cyber operation result in death, injury, physical damage, or destruction, it constitutes an armed attack[196]

To better understand what type of cyber attacks would be more likely to constitute an armed attack with regard to Article 51 UN Charter, it is useful to explore some examples. The hypothetical scenarios can be outlined, inclusive of 'fatalities caused by the loss of computer-controlled life-support systems; an extensive power grid outage (electricity blackout) creating considerable deleterious repercussions; a shutdown of computers controlling waterworks and dams, generating floods of inhabited areas; deadly crashes deliberately engineered (e.g., through misinformation fed into aircraft computers)' and 'the wanton instigation of a core-meltdown of a reactor in a nuclear power plant, leading to the release of radioactive materials that can result in countless casualties if the neighbouring areas are densely populated'[197]. The above-mentioned cyber attacks all have one thing in common: they result in physical effects. By contrast, a cyber attack arising out of the mere destruction, damage, or alteration of data can hardly be recognized as an armed attack. For instance, 'acts of mere cyber-intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services'[198], do not qualify as armed attacks.

Some scholars as well as states however favour more expansive view which qualifies cyber attacks impairing the national interest of a state as an armed attack regardless of whether the consequences are physical or non-physical. Indeed, Constantinou proposed a definition of the scale and effects standard by maintaining that an armed attack is 'an act or the beginning of a series of acts of armed force of considerable magnitude and intensity (i.e.. scale) which have as their consequences (i.e.. effects) the infliction of substantial destruction upon important elements of the target State, namely, upon its people, economic and security

[194] Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), ICJ Reports 2003, paragraph 72.
[195] SCHMITT, Michael N. Cyber Operations and the *jus ad bellum* Revisited. Villanova Law Review, 2011, p.589.
[196] Id, p.589.
[197] DINSTEIN, Yoram. Computer Network Attack and Self-Defene. International Law Studies, US. Naval War College, 2002, Vol.76, p.105.
[198] Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 71, pp.339-348.

infrastructure, destruction of aspects of its governmental authority, i.e.. its political independence, as well as damage to or deprivation of its physical element namely, its territory', and the 'use of force which is aimed at a State's main industrial and economic resources and which results in the substantial impairment of its economy'[199]. Unlike Dinstein, Constantinou is of the view that not only cyber attacks causing physical damage potentially amount to a use of force, but also those that severely incapacitate critical infrastructures so as to affect state security. Joyner also seems to prefers the extensive approach. He argued that the cyber attacks committed to steal data or disrupt air traffic control resulted in shutting down a state's air traffic control system, as well as in collapsing banking institutions, financial systems and public utilities, severe enough to constitute an armed attack[200]. He further contended that the nature of the target being attacked (such as information stolen or compromised are considered vital to national security) plays a role in determining whether an action qualifies as 'armed attack'. For instance, if a foreign government attacks the computer databases of another state's department or ministry of defence, and steal classified information related to troop locations during a time of conflict, or the codes to nuclear weapon's launch instrument, such actions could qualify as being tantamount to 'armed attack', even though no immediate loss of life or destruction results[201]. Especially noteworthy in this regard was the June 2018 statement by the Dutch Minister of Defense, AnkBijleveld, in which she stated, 'if a cyber-attack targets the entire Dutch financial system or if it prevents the government from carrying out essential tasks such as policing or taxation…it would qualify as an armed attack. And it would thus trigger a state's right to defend itself, even by force'[202].

With regard to current international law *jus ad bellum*, it would be not reasonable if we conclude that all cyber attacks affecting infrastructure functionality but not resulting in material damage meet the high scale and effects threshold of an armed attack. It is because of some reasons. Firstly, the UN Charter's articles traditionally focus on physical destruction and fatalities do not cover those attacks that do not result in physical consequences, or more specifically, serious physical destruction or death. Hence, cyber-attacks causing no physical harm cannot be considered to meet the requirements of an armed attack. Secondly, the

[199] CONSTATINOU, Avra. The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter. Athens and Bruxelles: Ant N Sakkoulas/Bruylant, 2000, pp 63-64.
[200] Id
[201] Id
[202] SCHMITT,Michael N. Estonia Speaks Out on Key Rules for Cyberspace. Available at https://csrcl.huji.ac.il/blog/estonia-speaks-out-key-rules-cyberspace

prevailing view is that Article 2(4) does not concern economic force, then the cyber attacks that cause severe economic consequences will fall far from the ambit of Article 2(4). Thirdly, in the Nicaragua judgment, the ICJ distinguished between an armed attack and a 'mere frontier incident'. Concerning the nature of the acts, such as mere disruptions or destructions of the information infrastructure, communications and digitized services without causing human casualties or significant destruction of property, mere impairment of network systems of critical national and/or private infrastructure, manipulation of a stock exchange system and so on, they are merely unfriendly acts, or transgressions of international law[203]. The characteristic of these events is that they do not entail sufficiently grave consequences. Hence their scale and effects are unlikely to be sufficiently grave to warrant classifying them as an 'armed attack' within the meaning of the Charter. They are also solely series of cyber incidents that individually fall below the threshold of an armed attack although these attacks could indeed have far-reaching consequences for a state's interests. Cyber attacks will therefore only constitute an armed attack according to the UN-Charter if their effect meet the scale and degree of gravity necessary in another state's territory[204].

This issue was mirrored in practice with regard to the cyber attacks in Estonia, Georgia and Iran. The cyber attacks in Estonia and Georgia were mostly distributed by the method denial-of-service attacks[205] that disrupted critical electronic systems without causing significant and extensive physical damage. Interestingly, several DDoS attacks occurred before the Estonia and Georgia attacks were not classified as armed attacks. Denial-of-service attacks are unlikely to reach the threshold of an armed attack due to the established practice of not designating them as 'armed' together with the nature of their consequences[206]. Contrary to the cases in Estonia and Georgia, the Tallinn Manual was of the view that the Stuxnet operations against Iran's nuclear centrifuges reached the armed attack level because the computer virus caused physical damage to the centrifuges. This argument is strongly supported by some experts, for example Stavridis believes that there is no need to beg the

[203] DINSTEIN, Yoram. Computer Network Attack and Self-Defene. International Law Studies, US. Naval War College, 2002, Vol.76, p.105.
[204] PANGRAZZI, Sara. Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, Policy Brief. ICT for Peace Foundation, Geneva, 2021, pp.5-21.
[205] WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). The Yale Journal of International Law, 2011, Vol.36, p.423.
[206] HAYWARD, Ryan J. Evaluating the 'imminience' of a cyber attack for purposes of aticipatory self-defence. Columbia Law Review, 2017, Vol.117, p.412.

question of whether Stuxnet constituted an armed attack, because Stuxnet produced a destructive effect which normally associate with attacks in other domains[207].

As mentioned above, mere cyber incidents that do not produce grave effects can not amount to armed attacks. However, the case of cyber operations that do not result in injury, death, damage, or destruction, but that otherwise have extensive negative effects, remains unsettled. A typical example is a large-scale cyber attack that shuts down critical infrastructure such as the financial market for a long period and paralyzes a state's economy or causes the collapse of the national currency[208] or a cyber incident directed against a major international stock exchange that causes the market to crash[209]. This is a controversial problem that Tallinn Manual 2.0 mentioned in the Rule 71. Although there are no actual or potential fatalities, casualties or physical damage in these events but the consequences are long-lasting, catastrophic, severe and harmful for the state's stability. It is because 'the law is ambiguous as to the precise point at which the scale and effects of harm caused by a cyber operation will qualify it as an armed attack'[210].

4.2.2. Cyber attacks as an armed attacks by non-States actors

As has been said in Chapter 2, cyber attacks can be launched not only by States but also by non-state actors. Practically, similar to international terrorism, the majority of cyber operations against states are conducted by individuals and groups[211]. Previous discussion has centered around state actors, but due to the unique circumstances and the novel feature of cyber operations, the following question should be raised: 'Could a cyber attack carried out by a non-state actor from abroad be treated as an armed attack under Article 51 (assuming that the condition of scale and effect is sufficient)?'[212]

The debate over whether acts of non-State actors can constitute an armed attack absent involvement by a State remains controversial. Traditionally, Article 51 and the customary international law of self-defence were characterised as applicable solely to armed attacks undertaken by one State against another. In this respect, the UN Charter does not itself

[207] STAVRIDIS, James G. Incoming: What Is a Cyber Attack?.
Available at https://www.afcea.org/content/incoming-what-cyber-attack
[208] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.74.
[209] Talliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 71, pp.339-348.
[210] Id, pp-339-348.
[211] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.80.
[212] BURKADZE, Khatuna. A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace. The Fletcher Forum of World Affairs, 2020, Vol. 44, No. 1, p.44.

expressly contemplate non-state actors in the context of the rules on the use of force. The reason is that the Charter's drafters did not envisage that non-State actors would be able to conduct attacks with consequences comparable to those of states. Kinetic attacks by non-state actors generally fell within the scope of criminal law and law enforcement paradigm if the attack came from within its own territory.

In modern academics, there are two approaches concerning this issue. The former maintains that there exists a primary rule of international law providing for a right of states to use force in case of an armed attack, whoever the author[213]. Supporting this approach, some scholars agree that whereas Article 2(4) of the Charter refers solely to State actors on both sides, Article 51 mentions a State only as the potential target of an armed attack, not the perpetrator[214]. The latter approach derived from "safe-haven" doctrine, which attributes armed attacks by non-state actors to the state from where they originate if this state is unable or unwilling to prevent or terminate the attacks[215]. In the cyber context, this doctrine seems not to be promising because cyber attacks are very difficult to attribute to a state. Even if cyber attacks can be tracked to a certain territory, it is not clear whether there is actually a state sponsor of the attacks. The nature of cyber attacks is anonymous, thus adversaries can route their attacks through other's computer systems. As a result, it may be very difficult to link a penetration or disruption of a computer or information networks to the responsible party[216].

However, the 9/11 attacks by Al Qaeda originating from across the border beg the question of whether they amount to an armed attack within the meaning of Article 51. The international community characterised the 9/11 attacks by Al Qaeda on the United States as an armed attack triggering the inherent right of self-defence. Indeed, the Security Council reaffirmed the inherent right of individual and collective self-defence of the United States with regard to the 11 September 2001 by adopting numerous resolutions, such as Resolution 1368 on 12 September 2001, Resolution 1373 on 28 September 2001. International organisations such as NATO and many individual States took the same approach. The North

[213] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.80.
[214] DINSTEIN, Yoram. War, Agression amd Self-Defence. 5th edition. Cambridge: Cambridge University Press, 2011, p.225.
[215] TAMS, Christian J . The Use of Force Against Terrorists. European Journal of International Law, 2009, vol.20, issue 2, p. 385; PANGRAZZI, Sara. Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, Policy Brief. ICT for Peace Foundation, Geneva, 2021, p.17.
[216] WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). The Yale Journal of International Law, 2011, Vol.36, p.444.

Atlantic Council determined that the attack on 9/11 against the United States shall be regarded as 'an armed attack against one or more of the Allies in Europe or North America' and therefore the right to self-defence should be invoked[217].

Besides, in the wake of the 9/11 terrorist attacks on the United States, such state behavior tends to indicate that states are willing to resort the right of self-defense against attacks perpetrated by non-state actors. During 2002, Russia in invoking its right of self-defence, conducted armed operations against Chechen rebels and accused Georgia of failing to prevent the terrorist attacks[218]. In the 2006, Israel launched its operations in self-defence against Hezbollah (non-state terrorists) militias based in southern Lebanon. Many states supported the position of Israel regarding to the right of self-defense against such attacks[219]. Similarly, in February 2008 Turkey launched a full-scale troop into northern Iraq in response to attacks by the Kurdish Workers' Party (PKK) which was operating from here. However, this action was not condemned by the UNSC[220]. The Netherlands also argued that both states and non-state actors can carry out an armed attack, including by cyber means, that entitles the victim state to self-defence.[221] The trend in State practice clearly shows that non-state entities could be armed attacks justifying the right to self-defence. It is also worth noting that Tallinn Manual 2.0 put forward the question of whether a cyber attack conducted by a non-state author shall be treated as an armed attack. Based on State practice, a majority of the International Group of Experts concluded that the answer was positive. The practice of states has established a right of self-defence in the face of cyber operations at the armed attack level by non-State actors acting without the involvement of a State, such as terrorist or rebel groups[222].

Nevertheless, cyber attacks carried out by non-state entities do not qualify as armed attack unless they are assessed in conjunction with the degree of force. As Gill emphasised 'it is not so much who is carrying out the use of force, but what the scale and effects of such an operation are - which is important in determining whether the operation constitutes an "armed

---

[217] NATO. Statement by the North Atlantic Council on 12 September 2001. Press release. Available at https://www.nato.int/docu/pr/2001/p01124e.htm#:~:text=More%20specifically%2C%20they%20condemned%20terrorism,international%20commitments%20and%20national%20legislation.

[218] HENDERSON, Christian. The Persistent Advocate and the Use of Force: The Impact of the United States upon the Jus ad Bellumin the Post - Cold War era. Routledge Taylor & Francis Group, 2016, p.160.

[219] Id, p.162.

[220] Id, p.163.

[221] ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, p.84-85.

[222] Taliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 71, pp.339-348.

attack" '[223]. At this corner, we can refer to the Ruys's proposal[224] when considering those cyber attacks from non-state actors. According to Ruys they can qualify as such only if they cumulatively fulfill these conditions: 1) the attack has to be large-scale, or it has to be a prolonged campaign of less substantial attacks, 2) there has to be a link to the State on whose territory self-defence is to be performed and the attacks are coming from non-State military-like group, 3) there is a strong evidence that future attacks are imminent, 4) the State on which the non-State actors reside is unwilling to take action to prevent further attacks, 5) non-State actors cannot be dealt with in any other means, 6) the defensive action is only targeted against non-State actors and is in accordance with proportionality of the attacks.

4.2.3. Anticipatory self-defence against pre-emptive cyber attacks

Chapter 2 introduces anticipatory self-defense in general, however this part moves on to the question of how to theoretically evaluate when a cyber attack is 'imminent' for purposes of anticipatory self-defense. In the cyber context, the issue of anticipatory self defense remains a controversial aspect. Actually, the nature of cyber-attacks seems to match very well with the 'imminent, overwhelming, leaving no choice of means, and no moment for deliberation' requirements of the Caroline doctrine because the speed of a cyber operation, once launched, usually precludes an opportunity to preempt the incoming attack effectively[225].

Tallinn 2.0 has endorsed the doctrine of anticipatory self-defence in the cyber context. In Rule 73, it quotes:

> *The International Group of Experts took the position that even though Article 51 does not expressly provide for defensive action in anticipation of an armed attack, a State need not wait idly as the enemy prepares to attack. Instead, a State may defend itself once an armed attack is 'imminent'. Such action is labeled 'anticipatory self-defence' in international law. This position is based on*

[223] GILL, Terry D. The Law of Armed Attack in the Context of the Nicaragua Case. Hague Yearbook of International Law 1, 1988, p.50.
[224] RUYS, Tom. Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practice. Cambridge: Cambridge University Press, 2010, pp. 531-532.
[225] HAYWARD, Ryan J. Evaluating the 'imminience' of a cyber attack for purposes of aticipatory self-defence. Columbia Law Review, 2017, Vol.117, p.414.

the standard of imminence articulated in the nineteenth century by US Secretary State Webster following the Caroline incident[226].

However, this part argues that the right to anticipatory self-defence and the effect-based model find difficulty to have dual existence under temporally international law. There are two main reasons that support this argument.

Acepting the effect-based approach for the event of cyber-attacks, the answer depends on the consequences of an action. In case of anticipatory self-defence, no actual attack occurs and thus there are not actual effects to measure. As a result, the effect-based approach cannot be applied to justify an action of anticipatory self-defence. Even if the future cyber-attacks threaten significant loss of life, destruction of property or lasting economic damage, the strict textual reading of Article 51 does not allow for threat of use of force.

Furthermore, to exercise the right to pre-emptive self-defence, the victim State must have concrete reason to believe that the adversary intends to carry out an attack in the near future. In this regards, the intentional damages approach seems to be more reasonable than effect-based approach since the latter only pays attention to the aftereffects of an actual attack.

Amongst a number of analysists noted, the main question is not whether a cyber attack constitutes an armed attack, but rather whether a cyber attack with a specified effect amounts to an armed attack. If both the direct and indirect effects to be produced by a cyber attack would cross the *de minimis* threshold of an armed attack in the sense of Article 51 of the UN Charter (effect and scale), it is likely that the cyber attack would be treated as an armed attack, justifying self-defence in response.

[226] Talliin Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, Rule 73, p.350.

CONCLUSION

The appearance of Stuxnet and several attacks in Estonia, Georgia marked the beginning of a new era for cyber attacks and new evolution of armed conflict in the world. These developments of technology definitely challenge the framework on the use of force, particularly in the absence of specific *jus ad bellum* rules applicable to cyber attacks. There are many uncertainties regarding the applicability of existing international law to cyberspace, one of which is the question of whether a state may respond in self-defense to a cyber operation.

In light of the foregoing, it is critical to define fundamental dimensions of cyber attacks based on clarification of term 'force' and 'armed attack' in Article 2(4) and Article 51 respectively. First, an armed attack represents legal grounds for the use of an individual or collective defense mechanism. Second, the right to self-defence under Article 51 of the Charter may be exercised against a cyber attack only to the extent that it qualifies as a most grave form of the use of force (an 'armed attack'). Therefore, interpretation of Article 51 of the UN Charter has been expanded to encompass cyber attacks as armed attacks. Third, if we adopt the dynamic meaning of armed attacks, the scope of cyber attacks should not be limited to the only perpetrator, namely a state actor. Since Article 51 of the UN Charter does not place any limitations on an originator carrying out an armed attack, non-state entities should be recognized.

This thesis supports the view that the effect-based approach is the most promising method at the present in determining when and if a cyber operation qualifies as the gravest form of use of force (armed attack). This approach is heavily reflected in the Tallinn Manual 2.0, which accepts that 'scale and effect' are qualitative and quantitative factors that would apply in this case. According to Tallinn Manual 2.0, cyber attacks rise to the level of an armed attack if they cause injury or death to persons or damage or destruction to objects. It should be read that at least cyber attacks with lethal results or significant property damage do indeed cross the threshold of an armed attack and hence can justify self-defence on the basis of Article 51 of the UN Charter.

Bibliography

Book

1. BRENNER, Susan W. Cyber threats: The Emerging Fault Lines of the Nation State. 1st Edition. Oxford University Press, 2009, 320p.
2. CLARKE, Richard A, KNAKE, Robert K. Cyber War: The Next Threat to National Security and What to Do About It, 2010, 320p.
3. CONSTATINOU, Avra. The Right of Self-Defence under Customary International Law and Article 51 of the UN Charter. Athens and Bruxelles: Ant N Sakkoulas/Bruylant, 2000, 225p.
4. DINNISS, Heather Harrison. Cyber Warfare and the Laws of War. Cambridge University Press, 2012, 331p.
5. DINSTEIN, Yoram. War, Agression amd Self-Defence. 6th edition. Cambridge: Cambridge University Press, 2017, 405p.
6. FAIX, Martin. Law of Armed Conflict and the Use of Force. Palacky University, 2014, vol I, 115p.
7. GILL, Terry D. The Law of Armed Attack in the Context of the Nicaragua Case. Hague Yearbook of International Law, 1988, vol 1, p.50.
8. GRAY, Christine. International Law and the Use of Force. Oxford University Press, 2008, 3rd edition, 455p.
9. HENDERSON, Christian. The Persistent Advocate and the Use of Force: The Impact of the United States upon the Jus ad Bellumin the Post - Cold War era. Routledge Taylor & Francis Group, 2016, 207p.
10. KELSEN, Hans. Collective Security Under International Law. U.S. Naval War College: Newport, 1954, vol.XLIX, 281p.
11. NATIONAL RESEARCH COUNCIL. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington. DC: The National Academies Press, 2009, 360p.
12. POPESCU, Nicu, SCRIERRU, Stalislav (eds). Hacks, leaks and disruptions: Russian Cyber Strategies. European Union Institute for Security Studies, 2018, 125p.
13. ROSCINI, Marco. Cyber Operation and Use of Force. Oxford University Press, 2014, 307p.

14. RUYS, Tom. Armed Attack and Article 51 of the UN Charter: Evolutions in Customary Law and Practice. Cambridge: Cambridge University Press, 2010, 585p.
15. SCHMITT, Michael N.(ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare. Cambridge University Press, 2017, 598p.
16. SHAW, Malcolm N. International Law. Cambridge University Press, 2008, 6th edition, 1542p.
17. SIMMA, Bruno, MOSLER, Hermann et al. The Charter of the United Nations: A Commentary, 2rd edition. Oxford University Press, 2013, 895p.
18. TIKK, Eneken et al. International Cyber Incidents: Legal consideration. Cooperative Cyber Defence Centre of Excellence (CCD COE), 2010, 128p.
19. U.S. ARMY TRAINING & DOCTRINE COMMAND. Critical Infrastructure Threats and Terrorism. DCSINT Handbook No. 1.02, 2006, VII-2.

Book chapters

1. ZEMANEK, Karl. Armed Attack. Max Planck Encyclopedia of Public International Law, 2010, paragraph.21.
2. RANDELZHOFER, Albrecht. The Charter of the United Nations, a commentary, edited by Bruno Simmma, 3rd edition, volume I. Oxford University Press, 2012, p.1421

Scientific Journals

1. AZUBUIKE, Eustace Chikere. Probing the Scope of Self Defense in International Law. Annual Survey of International & Comparative Law, 2011, Vol. 17, Issue 1, Article 8, pp.129-183.
2. BARKHAM, Jason. Information Warfare and International Law on the Use of Force. Interntional Law and Politics, 2002, Vol.34, pp.57-113.
3. BURKADZE, Khatuna. A Shift in the Historical Understanding of Armed Attack and Its Applicability to Cyberspace. The Fletcher Forum of World Affairs, 2020, Vol. 44, No. 1, pp.33-48.
4. CHIEN Eric et al. W32.DuQu – The Precursor to the Next Stuxnet. Version 1.4. Symantec, 2011.

5. COHAN, John Alan. The Bush Doctrine and the Emerging Norm of Anticipatory Self-Defense in Customary International Law. Pace International Law Review, 2003, pp.283-351.
6. COX, Stephen J. Confronting Threats Through Unconventional Means: Offensive Information Warfare as a Covert Alternative to Preemptive War. Houston Law Review 42, 2005, pp.881-895.
7. DINSTEIN, Yoram. Computer Network Attack and Self-Defene. International Law Studies, US. Naval War College, 2002, vol.76, pp.99-119.
8. EVRON, Gadi. Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War. Georgetown Journal of International Affairs, 2008, no. 1, pp.121-126.
9. FOLTZ, Andrew, C. Stuxnet, Schmitt Analysis, and the Cyber 'Use-of-Force' Debate. Joint Force Quarterly, 2012, issue 64, pp.40-48.
10. HATHAWAY, Oona A. et al. The Law of Cyber - Attack. California Law Review, 2012, vol.100, pp.817-885.
11. HAYWARD, Ryan J. Evaluating the 'imminience' of a cyber attack for purposes of aticipatory self-defence. Columbia Law Review, 2017, vol.117, pp.399- 434.
12. HOLLIS, Duncan B. Why the State need an Inetrnational Law for Information Operations. Lewis and Clark Law Review, 2007, vol.11, pp.1024-1057.
13. JENSEN, Eric Talbot. Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Brigham Young University Law School, 2002, pp. 207-240
14. JONATHAN, Pan Juin Yang, FUNG, Chun Che. Artificial Intelligence in Malware - Cop or Culprit?. Murdoch University, pp.181-184.
15. JOYNER, Christopher C., LOTRIONTE, Catherine. Information Warfare as International Coercion: Elements of a Legal Framework. European Journal of International Law, 2001, Vol.12, No.5, pp. 825-865.
16. KRIFT, Thomas R. Self-Defense and Self-Help: The Israeli Raid on Entebbe. Brooklyn Journal of International Law, 1977, vol. 4, no. 1, pp. 43-62.
17. LINNAN, David K. Self-defense, Necessity, and U.N collective security: United States and other views. Duke journey of Comparative and International Law, 1991, pp.57-123.
18. MURPHY, Sean D. Terrorism and the Concept of Armed Attack in Article 51 of the U.N.Charter. Harvard International Law Journal, 2002, vol. 43, no. 1, pp. 41-52.

19. NGUYEN, Reese. Navigating 'Jus Ad Bellum' in the Age of Cyber Warfare. California Law Review, 2013, vol. 101, No. 4 , pp. 1079-1129.
20. PANGRAZZI, Sara. Self-Defence against Cyberattacks? Digital and Kinetic Defence in Light of Article 51 UN-Charter, Policy Brief. ICT for Peace Foundation, Geneva, 2021, pp.5-21.
21. RID, Thomas, MC BURNEY, Peter. Cyber weapon. RUSI Journal 157, 2012, No.1, pp.6-13.
22. ROSCINI, Marco. World Wide Warfare: Jus ad bellum and the Use of Cyber Force. Cyber Operations and the Use of Force in International Law. Offord University Press, 2014. pp.85-130.
23. SCHMITT, Michael N. Cyber Operations and the *jus ad bellum* Revisited. Villanova Law Review, 2011, pp.569-606.
24. SIMMONS, Noah. A Brave New World Applying International Law of War to Cyber-Attacks. Journal of Law & Cyber Warfare, 2014, Vol. 4, No. 1, pp.42-108.
25. STEPHEN, Herzog. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. Journal of Strategic Security, 2011, pp. 49-60.
26. TAFT, William. H. Self-Defense and the Oil Platforms Decision. The Yale Journal of International Law, 2004, vol.29, pp.295-306.
27. TAMS, Christian J . The Use of Force Against Terrorists. European Journal of International Law, 2009, vol. 20, issue 2, pp.359-397.
28. VALUCH, Jozef; HAMUĽÁK, Ondrej. Use of Force in Cyberspace. International and Comparative Law Review, 2020, vol. 20, no. 2, pp. 174-191.
29. VAN DE HOLE, Leo. Anticipatory Self-Defence Under International Law. American University International Law Review 19, 2003, no. 1, pp.69-106.
30. WATT, Sean M. Low –Intensity Computer Network Attack and Self-Defense. International Law Studies 87, 2011, p.70.
31. WAXMAN, Matthew C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). The Yale Journal of International Law, 2011, vol.36, pp.421-458.

Legal regulalations

1. Charter of the United Nations, San Francisco, 26 June 1945, in force 24 October 1945.
2. Declaration on Principles of International Law concerning Friendly Relations and Cooperation among States in accordance with the Charter of the United Nations, GA Res 2625 (XXV), 24 October 1970.

3. Declaration on the Definition of Aggression, GA Res 3314 (XXIX), 14 December 1974.
4. Declaration on the Enhancement of the Effectiveness of the Principle of Refraining from the Threat or Use of Force in International Relations, GA Res 42/22, 18 November 1987.
5. Resolution 1368 (2001) adopted by the Security Council at its 4370th meeting, on 12 September 2001.

Judgments

1. Advisory Opinion of The International Court of Justice of 8 July 1996, Legality of the Threat or Use of Nuclear Weapons.
2. Case concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), Judgment of 26 November 1984, ICJ.
3. Case concerning Oil Platforms (Islamic Republic of Iran v. United States of America), Judgment of 6 November 2003, ICJ.
4. Case concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment of 19 December 2005, ICJ.
5. The Corfu Channel case (United Kingdom of Great Britain and Northern Ireland v. Albania), Judgment of 9 April 1949, ICJ.
6. ERITREA-ETHIOPIA CLAIMS COMMISSION. Partial Award Jus Ad Bellum-Ethiopia's Claims 1-8. Report of International Arbitral Award, 2005, Vol. XXVI, paragraph 11, p.465.
7. Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion of 9 July 2004, ICJ.

Internet page

1. FRY, Maddy. Anonymous Launches New Cyberattack Against Israel. Available at https://time.com/51616/anonymous-israel-attack/
https://csrcl.huji.ac.il/blog/estonia-speaks-out-key-rules-cyberspace
https://www.nato.int/docu/pr/2001/p01124e.htm#:~:text=More%20specifically%2C%20they%20condemned%20terrorism,international%20commitments%20and%20national%20legislation

2. HUDDLESTON JR, Tom. What is Anonymous? How the infamous 'hacktivist' group went from 4chan trolling to launching cyberattacks on Russia. Available at https://www.cnbc.com/2022/03/25/what-is-anonymous-the-group-went-from-4chan-to-cyberattacks-on-russia.html
3. JAHN, George. Stuxnet virus penetrates nuclear plant, may cause Chernobyl-like disaster. Available at https://www.csmonitor.com/World/Latest-News-Wires/2011/0131/Stuxnet-virus-penetrates-nuclear-plant-may-cause-Chernobyl-like-disaster
4. NATO. Statement by the North Atlantic Council on 12 September 2001. Press release. Available at
5. SCHMITT,Michael N. Estonia Speaks Out on Key Rules for Cyberspace. Available at
6. STAVRIDIS, James G. Incoming: What Is a Cyber Attack?. Available at https://www.afcea.org/content/incoming-what-cyber-attack
7. What Is the Difference: Viruses, Worms, Trojans, and Bots?. Cisco Security. Available at https://tools.cisco.com/security/center/resources/virus_differences
8. BAKER, Stewart Baker, WATERMAN, Shaun Waterman, et al. In the Crossfire—Critical Infrastructure in the Age of Cyber War, 2009, p. 6. Available at http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf
9. TAMKIN, Emily. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for CyberThreats?. Available at https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/
10. EU Commission, Green Paper on a European Programme on Critical Infrastructure Protection, COM(2005) 576 final, 17 November 2005, p 20. Available at https://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2005:0576:FIN:EN:PDF

Other doccuments

1. Joint Terminology for Cyberspace Operations.
2. NATO's Glossary of Terms and Definitions, p 2–C–11.
3. Principle of International Law on the Use of Force by States in self-defence, Chatham House, 2005.
4. Rule 1(m), HPCR Manual.

5. US National Military Strategy for Cyberspace Operations, p GL–1.