Migration Letters

Volume: 20, No: S5(2023), pp. 954-966

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)
www.migrationletters.com

The Right of Legitimate Defense Against Cyberattacks in Public International Law

Dr. Amr Ezzat Mahmoud Elhaw[1]

Abstract

The emergence of this unusual occurrence necessitated the intervention of international law, which looked for to regulate it through the prohibition or discouragement of its employment through force, as expressed in Article 4/2 of the United Nations Charter, Additionally, international law aimed to govern the permissible usage of technology in the civil and military fields. This action was undertaken as a reaction to the recent increase in cyberattacks and the growing reliance in all fields This paper aims to analyse the legal criteria surrounding the classification of cyberattacks as acts of military aggression, specifically focusing on the circumstances requiring the use of the right to justified defence against governments and other powerful bodies.

Keywords: *legitimate legitimate- cyberattack- aggression-armed assault- justice-justification.*

1- Introduction

In accordance with the conditions outlined in the fourth paragraph of Article 2 of the UN Charter, the prohibition of using force or the mere threat thereof in matters relating to international relations is absolute, allowing for no exceptions. The aforementioned legislation has created a multitude of factors and criteria to determine the circumstances in which the use of force is considered permissible. The aforementioned statement aligns with the rules outlined in Chapter VII of the Charter, which indicate two situations in which the use of force is considered acceptable: self-defense conducted in good faith and the adoption of collective security measures by the Security Council in response to a perceived danger to international peace or security.

The concept of legitimate defence, which is both ancient and significant, has been an integral component of legal systems at the local, national, and international levels throughout history. Despite the existence of several legal frameworks that recognise it as an essential and instinctive entitlement, considerable discord and contention persist regarding this matter. The aforementioned factors, including the circumstances surrounding it, various expressions, evolving perceptions, and its intersection with other rights, contribute to the current debate on the validity and existence of this right. These elements have led to discussions focused around reaching consensus and establishing common ground. One of the foremost challenges that need thorough examination and analysis within the realm of international relations is the increasing use of technology and the emergence of new manifestations of violence.

[1] Police Science Academy-Sharjah, Department of Law and criminal sciences, United Arab Emirates, dr.amr.elhow.police@gmail,com, ORCD.NO.0009-0000-1254-2323

The existence of the right to legitimate defence is supported by the UN General Assembly's Resolution No. 3314 of December 14, 1974, which restricts the definition of aggression to acts committed by states. This is in line with Article 51 of the United Nations Charter, which states that the right for legitimate defence applies in the event of an armed force attack, without explicitly specifying whether the attacking entity must be a state or an armed group.

Consequently, for individuals to possess a legitimate right to self-defense against cyberattacks, it is imperative to classify such assaults as "armed assaults" and attribute their execution to governmental entities. This two-part investigation examines the evolution of the right to justified defence, focusing on the prerequisites that must be met in instances of aggression, as well as the potential consideration of electronic attacks as equivalent to armed assaults.The present paper aims to address many significant concerns. Please provide a more detailed explanation about the scope of a state's entitlement to engage in legitimate self-defense. Additionally, endeavour to address the central inquiry. Is the right to justifiable defence universally applicable in all instances of attack, or is it restricted to certain circumstances?

The aim of this article is to give more clarification on the conditions of exercising the right to legitimate defence against cyberattacks,, which is dependent upon these assaults being classified as armed attacks. Consequently, the study places significant stress on the right to legitimate defence, which is restricted from being exercised in the presence of various types of force or violence, including political or economic coercion. Moreover, the act of legitimate-defense must meet the criterion of being "sufficiently dangerous" to potentially cause bodily injury to individuals or property, or even result in loss of lives.

1-1-Principal questions

The study will try to answer some important questions.

What is the scope of the right to legitimate defence of states?

Is the right of legitimate defence available in all cases of assault, or is it restricted to certain conditions for its exercise?

What are the conditions for practicing and exercising the right to legitimate defence?

When can cyberattacks be considered crimes of aggression?

Are there cyberattacks that don’t amount to resorting to the right of legitimate defence?

1-2-Study Objectives

The study aims to clarify that exercising the right to legitimate defence against electronic attacks is contingent on these attacks constituting an armed attack, as previously explained. As a result, the study highlights the right to legitimate defence that cannot be exercised against various acts of coercion or violence, such as political or economic coercion, and that must also be "sufficiently dangerous" to cause physical damage to property or cause death.

2- Method

2-1-The concept of legitimate defense in the U.N.Charter

Although Article 51 of the Charter of the UN was drafted in a broad manner, eliminating specific identification of the perpetrator of an attack and asserting the right to etamitigel-defense in the case of an armed assault, it can be argued that a victim state possesses the right to use legitimate defence when electronic attacks meet the criteria of armed attacks as outlined in the Charter.

Consequently, regardless of the severity or lethality of collective or gang activity, it is not viewed as an antagonistic action. Therefore, as indicated in the aforementioned article, the term "state" in this particular context is used regardless of its recognition or participation in the UN. This definition also imposes limitations on the entitlement to defend against an attack perpetrated by either a state or a group of states. Moreover, as noted by the Court of Justice, the term "it" may be used to denote a group of states when deemed suitable. In instances when the court deems there to be a legitimate defence against a state's attack, the implementation of Article 51 of the Charter is warranted. Additionally, the Court of Justice has affirmed that this provision may be extended to a collective of nations if deemed essential. despite the provision outlined in Article (3/g) of the aforementioned ruling, which stipulates that the sending of gangs or entities consisting of armed, unregulated, or hired forces acting on behalf of or in representation of a nation and undertaking actions against another nation that possess a level of peril comparable to, among other things, a genuine armed assault by conventional forces.

According to the passage, a section of the regulations stipulated the potential occurrence of indirect aggression, in which numerous countries resorted to providing assistance, resources, or funding to armed factions to execute such actions on their behalf. This approach aimed to circumvent the prohibition on employing force or initiating an armed assault as outlined in Article 51 of the Charter of the UN (Ziolkowsky , Katharina , Stuxnet , 2012)

2-2: The right of legitimate defense in the International Court of Justice

In its evaluation of the military actions carried out by the Republic of the Congo (DRC) against Uganda, the International Court of Justice determined that the responsibility for the attacks launched by rebel groups did not lie with the DRC. Furthermore, the Court determined that it was not necessary for deliberation on the parties' disagreements regarding the recognition of the right to legal defence against assaults by unauthorised forces under contemporary international law, along with the specific conditions under which this right is necessary (Woltag christopher C./ Lotrionte Catherine , 2001)

In accordance with the General Assembly's Resolution No. 3314, that states that the aggressor must belong to a state, there exists an important inclination to examine the legality of using the right to legitimate defense against non-state actors. This examination extends to circumstances in which the act in question is not clearly attributed to a specific nation, and potentially even when it is. The principle of legitimate defence extends to instances of an imminent or ongoing military assault, regardless of whether the aggressor is a state or non-state entity. This stance has been expressly articulated by the US inside the context of cyberspace. This phenomenon might be attributed to the expansion and increased heterogeneity of these companies in relation to their resources and capabilities. In addition, the Netherlands has asserted that acts of armed aggression carried out by both state and non-state actors, including those using technological methods, are strictly prohibited(Wanger , Markus ,2013)

Due to the decision of the International Court of Justice, the evidence regarding Iran's participation in the removal of mines activities related to the oil platforms was deemed inconclusive. Similarly, the evidence indicating Iran's involvement for the assault on the city of Ayl was considered inadequate. In the legal dispute between the Democratic Republic of the Congo and Uganda, the International Court of Justice reiterated the need of providing "compelling evidence."

In the Corfu Strait case, the International Court of Justice highlighted the need for conclusive evidence that establishes a high level of certainty and eliminates any doubts when it comes to mine laying. However, it is important to note that the court did not specify a specific standard for evaluating military and paramilitary activities in this particular ruling. The Nicaraguan Court underscored the need of presenting compelling

evidence substantiating the prosecution's claims, while also evaluating the level of American control exerted on the "Contras."

It is important that several agreements specifically recognise the right to a legitimate defence against non-state actors. According to Article 4/5 of the 2006 Great Lakes Protocol on Non-Aggression and Common Defence, it stipulates that member nations are obligated to address instances of aggression. States and non-state entities possess the same ability to participate in acts of armed aggression. The prohibition of armed organisations using their territory for acts of aggression against armed organisations has been specifically stated by Member States. This prohibition is guided by the criteria outlined in Articles 6 and 8, as well as Article 2/8 of the Protocol (Talbot Jensen , Eric ,2017)

However, it is not possible to make this conclusion based on existing documents, including General Assembly Resolution No. 3314. Consequently, it can be believed that the exercise of the right to legitimate defence against cyberattacks carried out by non-state actors necessitates the fulfilment of two prerequisites: firstly, the conduct ascribed to this collective must qualify as an act of armed attack, and secondly, these actions must be attributable to a state, as previously articulated.

In instances when the armed forces of a state or any of its related organisations, agencies, or institutions are guilty for an act, the state may be held accountable. However, this principle does not apply when the crime is perpetrated by independent groups that lack formal affiliation. Furthermore, it is important to note that Article 8 of the drafted articles formulated by the International Law Commission pertaining to the issue of state responsibility for wrongful acts clearly asserts that the actions carried out by an individual or a collective entity may be attributed to a state.

In contrast, it is essential under international law that nations take measures to guarantee that individuals under their jurisdiction do not inflict damage upon other states, and that they duly hold accountable those individuals who are found accountable for such activities. This principle has been reinforced by the International Court of Justice in notable instances such as the Corfu Strait and kidnapping crimes (Reinhard Fabin , 2020)

If the committing of such acts is not attributed to a particular state, the state being victimised lacks a legal justification but retains the freedom to use law enforcement measures, both domestic and international, as well as collaborate with the violating state to request an end of such activities originating from their jurisdiction, or alternatively. restrict access to the internet as a means of reducing the cyberattack's impact.

In the event that the country from which this cyber assault originated is either unwilling or incapable of providing a response, maybe due to insufficient financial or technical resources, it becomes crucial for the targeted state to take action. In cases when armed attacks are exclusively perpetrated by non-state actors, it is essential that the defensive reaction be largely focused on these individuals rather than the state that harbours them.

According to the laws of both countries, it is imperative for states to exercise due diligence in order to avoid the use of their territory by other states or non-state actors for the purpose of engaging in military operations, including but not limited to planning, threatening, executing, or providing funding for armed actions against other countries or specifically Russia. It is vital to adhere to all essential measures in order avoid any infringements of the planned information security agreement. The agreement stipulates the need to combat any malicious activities conducted in the digital realm and effectively impede such cyberattacks (Natalino Ronzitti , 2006)

Based on the results of the UN Group of Governmental Experts in 2013, it was determined that the Union had established a set of principles for cyber peace, one of which emphasises the need for states to make efforts in preventing non-state actors from using their territory for illicit activities.

Due to the International Telecommunications Authority, the act of providing refuge to terrorists or criminals under its jurisdiction is considered unlawful. The modification to Rule 5 of the "Tallinn Handbook" included several viewpoints, in which it was stipulated that states are prohibited from intentionally allowing the use of electronic infrastructure within their jurisdiction or under their authority for commercial activities that have a detrimental and illegal impact on other countries.

In the Corfu Straits case, the International Court of Justice provided a decision stating that the attribution of awareness or responsibility to a state for an illegal act occurring throughout its territory or cannot be automatically assumed. The Court emphasised that the mere exercise of control over a state's territory and waters does not imply knowledge of the illegal act or the identity of the perpetrators. These facts are independent and distinct from other facts, and do not first imply any evident responsibility (Wanger , Markus , 2013)

(1) It is essential for nations to establish and enforce regulations and procedures that effectively eliminate safe havens for individuals who engage in illegal activities using information technology.

2-It is crucial for governments of all relevant jurisdictions to engage in collaborative efforts in the field of law enforcement, with the aim of investigating and punishing cases of global information technology misuse.

3-It is important for nations to engage in the sharing of information regarding the challenges they encounter in their efforts to combat the abuse of information technology.

4-Law enforcement agencies should have enough resources and instruction to effectively address instances of illicit use of information technology.

5-Legal systems have the responsibility to make sure that any violations of data availability, confidentiality, and integrity are met with appropriate punitive measures.

6-Legal systems are required to provide mechanisms that enable the efficient storage and retrieval of electronic data relevant to particular criminal investigations.

Rapid investigation and timely collection and transmission of evidence should be ensured through mutual aid mechanisms in order to address cases of information technology misuse effectively.

(8) The spread of knowledge to the general population about the critical significance of ceasing and resisting the utilisation of technology for illegal purposes is of utmost importance.

(9) It is essential to prioritise the development of information technology with the primary objective of assistance in the prevention and identification of unlawful activities, the tracking of perpetrators, and the acquisition of evidentiary material.

10-In order to ensure the proper use of information technology, it is essential to find a balance between preserving the efficacy of the criminal justice system and protecting privacy rights and individual liberties.The aforementioned steps include the fundamental elements of the necessary due diligence within the realm of internet (Michael N Schmitt, 2011/2012)

2-3: A side of the international practices

In the same vein, throughout the framework of international relations, the Security Council of the UN recognised the duty of the United States to exercise its right to individual or collective legitimate defence following the acts of aggression perpetrated by Al-Qaeda on September 11, 2001. Additionally, the Security Council acknowledged the activation of NATO mechanisms and the Rio Treaty as means of allowing collective legitimate defence in response to the mentioned attacks. Recent developments indicate an increasing endorsement of the right to engage in self-defense against armed assaults

committed by non-state entities, regardless of their non-Russian origin. In addition, the military campaigns conducted in 2002 to eradicate PKK strongholds can be observed, despite the absence of conclusive evidence implicating Iraq in supporting or being responsible for the activities of this armed faction. Kenya has further garnered backing for its military efforts against Al-Shabaab insurgents in Somalia through its reliance on Article 51 of the United Nations Charter (Mare Ellen O'connell , 2002)

3- Exercising the right of legitimate defense in international law

3-1-justifications of resorting to legitimate dfense

The examination of the circumstances, magnitude, and scope of the right to defence is vital to prevent its misuse, which may result in conflicts, heightened losses, and increased detrimental consequences. Instead, it is advisable to evaluate the circumstances, magnitude, and scope of the danger originating from the aggressor and attempt to reduce it.

Therefore, apart from the foregoing illegality and origin from either a state or a state-affiliated group, the act of defence necessitates adherence to several prerequisites. These conditions encompass the fulfilment of the criteria of necessity, proportionality, and immediacy, alongside the transient nature of the attacks. Furthermore, it is essential that the act of defence represents the only viable means of deterring an armed assault directed towards the state.

3-1: The Conditions of resorting to the Legitimate Defense

3-1-A: The act of defense is the only way to repel armed aggression.

This condition indicates that the act of defence is the only feasible and probable means to fend off this onslaught, rather than an alternative approach. This condition is commonly known as the "necessity" condition, as it requires that the use of armed force is the only viable option for preventing an attack, with the possible exception of the defensive action taken by the nation that has been attacked (or is facing an imminent attack in the case of pre-emptive legal defence) in exercising its right to legitimate self-defense.

Consequently, it is impermissible to engage in hostilities against another sovereign state or infringe against the impartiality of a country that is not involved in the act of aggression, demonstrated by Germany's transgressions against the neutralities of Belgium and Luxembourg as stipulated in the Treaties of 1839 and 1867. These activities are considered to be breaches of international law.

According to Article 51 of the text, it is obvious that the Security Council has the authority to take action in order to safeguard or restore global peace and security, without requiring a legitimate defensive reaction. On the other hand, in the event that the determined measure of defence against the armed assault proved to be ineffectual, it should not be inferred that it was unnecessary (Kimberly Amadeo , 2020)

3-1-B- the equality between the act of defense and the act of aggression

The use of legitimate defence is viewed as an exception to the ban on the use of force. Therefore, the act of defence must be limited to the extent required to overcome the ongoing attack. This condition relates to the correlation between the strategy used in defence and the means or act of assault. Some believe that it is possible to achieve a state of balance in terms of quantity. The decision to use armed force in a defensive capacity is dependent upon one of two factors: either an evaluation of the extent and consequences of an anticipated armed assault, or the objective of repelling such an attack. The prevailing perspective in jurisprudence often favours the adoption of the second standpoint, which posits that the use of force may be considered more imperative. The comparatively weaker force might have the capability to repel the assailant who is armed. From this

perspective, the concepts of proportionality and need intersect. Moreover, it is important to note that effective response does not need the use of a certain kind of weapon. The system facilitates both an electronic and kinetic response to a cyberattack, as well as a kinetic and electronic countermeasure.

FFor example, the potential for a cyberattack to be executed effectively may be restricted due to many factors. These factors might include the aggressor being a low-tech state or non-state actor that lacks the requisite digital infrastructure to carry out such an assault, or the victim state lacking the ability to engage in hacking activities. Forecasting of the extent and impact of cyberattacks is a tough task due to their rapidity and clandestine nature. Calculating proportionality in the cyber domain becomes difficult due to several factors. The assessment of proportionality is crucial in light of the interconnectedness of information systems, since unrestricted dissemination of deadly software across cyberspace might potentially occur due to the presence of biological weapons. In any given situation, an unbalanced reaction will just serve to attribute responsibility to the state for an exaggerated action or the improper use of self-defense, rather than transforming a lawful defensive measure into an unlawful act of retaliation. The proportionality of cyber reactions aimed at legitimate defence can be achieved when the programmes are specifically developed for this purpose. However, this necessitates a comprehensive understanding of the target systems, which can be acquired through conventional intelligence gathering, exploitation, or electronic espionage. The criteria of proportionality might be seen as primarily a technical matter. The concept of proportionality does not always entail the use of the most limited measures to address aggressiveness, halt it, or reduce its detrimental outcomes to the greatest extent possible (Kimberley N Trapp , 2011)

According to the 2011 Cyberspace Strategy, the United States has emphasised the importance of adhering to legal principles when responding to cyberattacks. Specifically, the use of force in self-defense against such attacks should be limited to the extent necessary for combating an ongoing or approaching armed assault, and it must be commensurate with the level of threat being confronted. This stance was articulated by the Deputy Secretary of Defence of the United States.

The Netherlands asserts that the use of force as a countermeasure to an armed cyberattack "should adhere to the prerequisites of necessity and proportionality." In accordance with the cybersecurity policy of Canada, it is stated that the scope of a cyberattack is a determining factor in selecting an appropriate course of action or measures for reaction and prevention (Karl Zenabek , 2012)

3-1-C- the availability of the immediacy.

This criterion is predicated on the idea that the principal objective of a legal defence is to repel the assault rather than exact retribution against the assailant. While the concept of quickness is subject to wide interpretation, it is important to note that it does not necessarily imply an instantaneous reaction.

Therefore, in the event that the state is deprived of its authority to engage in legitimate defence, it is imperative to minimise any unnecessary delay between an armed attack and the ensuing retaliatory action undertaken via legitimate defence. Considering its limited capacity for prompt response and the challenges associated with identifying the attacker's identity or origin, a considerable degree of flexibility is necessary when considering the timeliness of countermeasures, particularly in the context of cyberattacks. The target nation may experience a delay in its defensive response, whether in the form of electronic or physical measures. Additionally, the process of gathering sufficient evidence to attribute responsibility to a specific country or non-governmental entity may be time-consuming, especially in the case of cyber attacks. This assertion has particular weight in cases when the attack has successfully incapacitated the military computer systems and networks of the targeted state. The act of repelling or pushing back an assault that has

already begun may be seen as a kind of pre-emptive justified defence. This defensive measure aims to counteract an impending attack that is in the process of being started. Consequently, the state engaging in aggression forfeits its entitlement to a legitimate defence at the conclusion of the attack (J. F. R. Boddens Hosang and P. A. L. Ducheine , 2020)

3-1-D-the temporary nature of legitimate defense.

The temporary nature of defensive actions is essential to enable the Security Council return to its original authority and implement the necessary measures to cease the ongoing attack. The implementation of security measures is of utmost importance in the preservation of global peace and security. Once the Security Council takes responsibility and implements the necessary actions to protect global peace and security, the nation that has been wronged must give up its entitlement to legitimate -defense.

Therefore, there's a contention positing that the state's right to a valid form of legitimate -defense persists from the onset of an assault until the Security Council takes action in accordance with Article 51. However, worries have been raised over the potential forfeiture of the right to a justifiable defence as soon as the Security Council intervenes. If the Security Council is considered ineffectual or fails to fulfil its designated mission, does the state recover its right to legal defence, or is it only (Amer, Karim and Jehane Noujaim , 2019)

The dominant legal perspective was that, in the absence of Security Council engagement, the state was devoid of authority to use coercive measures. However, the entity possesses the legitimate authority to safeguard itself, even if an opposing party argues that its defensive actions are momentarily ineffective. In the event that the Security Council is unable to protect its interests in such a scenario, it becomes crucial, though essential, to clearly highlight the Council's incapacity by revealing the aggressor's refusal to comply with Security Council resolutions.

In the case of cyber attacks, nevertheless, the offending nation may initiate a military offensive for a restricted duration while awaiting a determination from the Security Council about further offensives (Heather Harrison Dinnis , 2012).

According to Article 51 of the United Nations Charter, it is mandated that governments promptly notify the United Nations Security Council of any actions undertaken in the pursuit of justifiable self-defense, whether on an individual or collective basis. Executing this specific stipulation might provide challenges in some circumstances owing to its clandestine nature and expeditiousness, including the legal guarding against cyber assaults. Therefore, the potential lack of sufficient time for preparation or notification of the Security Council may result in the rendered ineffectiveness of authorised defence measures. Does this indicate that failure to promptly inform the Security Council would render a lawful defence against a cyber attack invalid?

In the case concerning military and paramilitary activities in Nicaragua, the Court determined that the duty to report was not deemed customary international law, at least as of the time of the ruling. However, it could serve as one of the indicators to assess whether the state in question was confident in its adherence to its right to legal defence. However, the legality of exercising the right to legal defence remains unaffected, since Judge Schubel's separate judgement in the same case indicates that it would be contrary to the normal course of events if the necessity to adhere to this reporting condition enabled the perpetrators to act covertly. While it is true that individuals who engage in self-defense should not be penalised, it is important to acknowledge that a state has an inherent right to engage in individual or collective legitimate defence. This right should not be disregarded by failing to inform the Security Council about the measures taken in exercising this right (Banaszewska , Dorota Marianna , Lex Specialis , 2020)

In accordance with Article 51 of the United Nations Charter, which states that the use of legitimate self-defense requires certain conditions, it might be argued that defensive cyber operations are not intrinsically prohibited. In this particular scenario, it is important to note that the obligation of notice does not extend to technical information, including the techniques used, as well as the actions and policies of the aggressor state in a broader context (James A Green , 2009)

4- Cyberattacks that do not rise to the level of armed assault in international law.

4-1: The low-intensity cyberattacks

The most common kind Instances of cyber assaults against nations such as Estonia in 2007, Georgia in 2008, and Iran in 2010 are notable due to their intentional destruction of vital infrastructure. Nevertheless, the absence of significant harm suggests the occurrence of an armed attack. Consequently, it may be argued that low-intensity cyberattacks can be classified as a kind of cyberforce used by various nations. Due to a multitude of benefits, such as reduced expenses, simplified implementation, less likelihood of mass victimisation or its absence, and the ability to delay economic and social repercussions.

Thomas Frank's analysis of Article 5(1) of the United Nations Charter highlights the insufficiency of its scope in addressing contemporary inter-state conflicts, since they often fall short of meeting the threshold of armed aggression. Due to his viewpoint, cyberattacks that do not meet the criteria of an armed assault are not governed by the rules outlined in the United Nations Charter (Hamadoun l Toure , 2011)

The International Court of Justice determined that the use of force that does not constitute armed aggression allows the victim state to only respond with proportionate, non-coercive countermeasures in the case of the oil platforms, whereas in the case of the oil platforms, Judge Simma adopted a different point of view in his separate opinion and suggested differentiating between legitimate defense through the meaning of the article (5)

Nevertheless, this point of view has been subject to criticism by several legal scholars. The concept of proportionality is already relevant to legitimate defensive actions. However, as stipulated in Article 51 of the Charter, the use of force is only permissible in response to acts that meet the criteria of an armed assault. Consequently, engaging in such actions would be considered a violation of the Charter's provisions, as it is clearly prohibited.

Consequently, the threat of political or economic aggression, the presence of a danger to the lives and property of a nation's inhabitants in a foreign country, or a harm to the state's economic interests should not be deemed a prerequisite for engaging in military aggression. However, the victimised state has the right to respond with reciprocal measures. Therefore, cyberattacks that fail to meet the threshold of armed aggression do not confer upon the victim state a right to justifiable defence or the use of force (Christian J Tams , 2009)

Consequently, the injured state is obligated to engage in collaboration with cyber countermeasures and adhere to the regulations outlined in Chapter II of the draught articles on the responsibility of states for internationally unlawful behaviour, established by the International Law Commission. These articles are reflective of established customary international law. With the sole exception of "emergency countermeasures," it is essential for states that are impacted to duly notify the affected states on their intention to undertake countermeasures, while also extending an invitation to engage in discussions with the representative of the state concerned.

4-2: The probability of a Security Council intervention

despite the classification of cyberattacks as armed attacks, the nation that was impacted or any other United Nations member has the freedom to present the issue to the Security Council in accordance with Article 35 of the United Nations Charter. This article affirms the entitlement of each member to quickly refer urgent matters to the Security Council.

As stated in Article 36/1, the Council possesses the authority to propose appropriate procedures and methods for the resolution of disputes. In the event that the Council determines that the situation in question poses a threat to peace, a breach of peace, or an act of aggression, it is also empowered to exercise its jurisdiction as outlined in Chapter VII of the Charter (Governo italiano ,2012),

In evaluating the potential danger to peace, it is necessary to take into account many factors such as the degree of the violation, the specific rule that has been violated, the importance of the violation, and the potential international consequences it may entail. As an example, the United States Department of Defence argues that a cyber attack on a computer network that leads to extensive harm, economic disruption, or loss of human lives might potentially justify the initiation of Security Council measures. Iran presents a another instance of a cyberthreat to global peace, as it has formally urged the Security Council to intervene in cases when nations engage in disruptive cyberattacks against legitimate nuclear facilities. Nevertheless, there has been a concern that in the event of identification, computer assaults occurring amongst prominent Western economic countries, such as instances of economic espionage, may not be seen as a threat to global peace.

Therefore, in the event that the Security Council deems the cyber operation to be an act of aggression, a breach of international law, or a menace to the Muslim community, it has the authority to use its powers as outlined in Chapter Seven of the Charter. Whether via proactive measures to mitigate the escalated nature of the issue as stipulated in Article (40), or by providing guidance as outlined in Article (39). The implementation of measures prepared in accordance with Articles (41) and (42) has more significance. According to Article 41, the Council has the authority to propose or determine measures that include several aspects, including but not limited to the discontinuation of economic ties, restrictions on transportation methods such as land, sea, and air, as well as communication channels such as postal, telegraphic, wireless, and other means. Additionally, the Council may also choose to break diplomatic relations.

In light of activities that pose a threat to international peace, the Security Council has the authority to issue permission for Member States of the United Nations or United Nations peacekeeping forces to engage in cyber operations that are comparable to the use of force (Gray Chiristin , 2018)

Through this specific framework, the General Assembly has consistently expressed concern over the use of electronic technology in methods that are inconsistent with the preservation of worldwide peace and security.Hence, in accordance with prevailing conventions, the principle of legitimate defence is typically applicable solely to armed cyberattacks, while alternative measures or referral to the Security Council are deemed appropriate for addressing other forms of aggression. In light of Article 51 of the United Nations Charter, the decision to invoke the right to preemptive lawful defence against non-armed cyberattacks necessitates consideration of three key factors.

With the recognition that the cyberattack represents an inevitable stage of the approaching assault, the defender's response to the attack itself is the only option for effectively resisting it.

The second point. Electronic operations are considered to be one of numerous kinds of assaults that satisfy the criteria for being categorised as an armed attack (Elaine M Grossman , 2009)

III. A cyber attack or electronic operation that does not meet the requirements for an armed assault in isolation, and thus cannot justify the application of the right to legitimate defence on an individual level. However, it is essential to note that such attacks are part of a series of electronic strikes that together constitute an armed assault. The adoption of the "event track theory" in the context of periodic, small-scale attacks carried out by armed groups is now gaining recognition within legal circles (Eddy Melissa / Perlroth Nicole , 2020)

Kenya, as an illustrative case, seems to have used the concept of event accumulation in its identification of nine incidents spanning from 2009 to 2011. These incidents included various events, such as the incursion of the Al-Shabaab movement into Kenyan territory from Somalia. However, the position of Kenya over this subject encountered opposition. The behaviour and outcomes of the youth movement's invasions, which are likewise a subject of controversy, do not exhibit any discernible pattern. Additionally, Despite potential instability in the border region and potential financial losses resulting from attacks on tourists, significant material damage did not occur as a result of these raids or assaults. However, it is important to note that criticism aimed mainly at this aspect. Instead of concentrating just on the concept itself, it is important to examine whether the necessary conditions for the application of the theory of cumulative occurrences are satisfied (Dorr , Oliver , 2019)

Although the International Court of Justice has so far refrained from taking a firm stance on this issue, the court declined to issue a ruling based on the cumulative theory of events in the Cameroon v. Nigeria case on the grounds that "neither side sufficiently proves the facts he claims or attributes them to the other party

5- Conclusion

Based on the foregoing, we conclude that only online assaults that meet the legal definition of "armed assault" are permissible against the right to effective defense. Cyberattacks without the use of military forces may still result in a reaction, just as other assaults without the use of armed forces can be met with retaliation, non-coercive countermeasures, or a referral to the UN Security Council.

The International Court of Justice determined in the case of military and paramilitary actions in Nicaragua that the court has the right to apply exceptional criteria in each instance independently and not always in the same way, as long as it stays within the parameters of its law and regulations. One could argue that no universally accepted level of proof is required to establish globally unlawful activities under the purview of international law.

The legitimate defense only applies to armed aggression committed by a state or a group of states; however, an attack originating from gangs, armed groups, irregular forces, or mercenaries sent by a state can be considered an armed attack, provided that the designation of an act as an armed attack committed by the state itself in this situation is dependent on the requirement that this act be attributed to a state.

The Tallinn Directory did not address the standards of proof required in the context of cyberspace. The seventh rule said that just starting an electronic operation or getting it started in some other way through a government's electronic infrastructure is not enough proof to link the operation to that country. Rules (7) and (8) are the only rules that talk about proof.

- The state that invokes the defense must demonstrate, on the one hand, that the cyberattack occurred or is about to occur and that it caused enough significant injury or is reasonably expected to inflict enough damage to constitute an armed assault.

On the other hand, it is assigned to a certain state, either directly or via a group whose activities are attributed to a specific state.

- As a result, given the availability of clear and convincing evidence on allegations related to the use of force in international relations and given that the legitimate defense is an exception to the prohibition on the use of force, the standard of evidence must be higher to prevent violations of this rule.

- When a state invokes its right to legal defense against armed attack, charges of violations of the Law on the Legality of Force need "clear and convincing evidence" to justify the military action performed by the state that claimed its right to legal defense.

4: It should be noted that current international circumstances make it inappropriate to limit the right to legitimate defense against armed assault from sources other than the state or the organisations or troops it dispatches. Perhaps the inclusion of this criterion in United Nations General Assembly Resolution No. 3314 of 1974 reflects the lack of foresight at the time that armed groups would be able to cause harm on a par with state military forcible entry.

References

Amer, Karim and Jehane Noujaim (2019). In "The Great Hack."Video of a Netflix Original Documentary.Via Google Scholar

Banaszewska, Dorota Marianna , Lex Specialis (2020) , Max Planck Encyclopedia of public international law

Christian J Tams (2009) The Use of force against terrorists , European journal of international law

Dorr, Oliver (2019) Use of force , probibition of , Max Planck Encyclopedia of public internationl law

Eddy Melissa / Perlroth Nicole (2020) Cyber Attack Suspected in German Woman’s Death , The New York Times

Elaine M Grossman (2009) U.S. General Reserves Right to use Force , Even Nuclear , in Reponse to Cyber Attack , Global Security Newswire

Gray Chiristin (2018) , internationl law and the use of force , 4th ed . (Oxford : Oxford University)

Governo italiano (2012), La posizione italiana sui principi fondamentali di internet

Hamadoun l Toure (2011) the international response to cyberwar , in the quest for cyber peace edited by Hamadoun l Toure et al , ITU

James A Green (2009) Fluctuating evidentiary standards for self-defense in the international and comparative law quarterly

Heather Harrison Dinnis. (2012). Cyber Warfare and the Laws of War.Cambridge University Press, New York, NY.

J. F. R. Boddens Hosang and P. A. L. Ducheine (2020) "Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defense in the Face of Modern Threats."No., Amsterdam Law School Research Papers.

Karl Zenabek (2012) Armed attack , Max planck Encyclopedia of public international law , Volume1

Kimberley N Trapp (2011) State Responsibility for international Terrorism , Oxford University

Kimberly Amadeo (2020) How Today's Economy Is Affected by the 9/11 Attacks.

Mare Ellen O’connell (2002), lawful self-defense to terrorism , univesity of pittsburgh law review

Michael N Schmitt(2011/2012) cyber operations and the revisited , villanova law review

Natalino Ronzitti (2006) The Expanding Law of Self-Defense , journal of conflict and secruity law

Reinhard Fabin (2020) Der digitale Gegenangriff ist Keine brauchbare Strategie fur die Cyber-Vertei-digung , NZZ

Talbot Jensen , Eric (2017) The Tallinn Mannual 2.0 : Highlights and insights , Georgetown journal of internationl law , vol . 48 , 2017

Wanger , Markus (2013) Non -State Actors , Max Planck Encyclopedia of public international law,

Woltag christopher C./ Lotrionte Catherine (2001) information Warfare as international coercion: Elements of a Legal Framework , 12/5 European journal of internationl law

Ziolkowsky, Katharina , Stuxnet (2012) Legal considerations , The NATO cooperative Cyber Defense centre of Excellence