Ilkogretim Online - Elementary Education Online, 2019; Vol 18 (Issue 4): pp. 2231-2247
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2019.641217

The Law Of Self-Defence In Cyber Operations

Mian Muhammad Sheraz , Ph.D Law candidate in Department of law, International Islamic University, Islamabad, Pakistan and currently working as a Vice principal Mardan Law College, affiliated University of Peshawar. Email Id: sheeji333@gmail.com

Dr. Fazli Dayan , Assistant Professor in department of Shariah & Law, Islamia College University, Peshawar.

Abstract

Self-defence against cyber attacks can be practiced by physical, electronic or digital methods or means. Actual self-defence utilizes conventional weapons to focus on the digital infrastructure of the intruder, for example, the hosts, "servers" from which the digital attacks arise, or other actual targets consistently with the prerequisites of need and proportionality and with international humanitarian law. Electronic responses to a cyber attacks utilize "the employment of electromagnetic energy, directed energy, or antiradiation weapons to attack forces , installations, or instruments with the purpose of debasing, negating, or obliterating enemy fighting capacity. Cyber defences can be latent or dynamic. While latent safeguards don't include pressure or unapproved interruption into PC systems and hence are not a use of force, the latter are reactions in-kind to a past cyber attack and are indeed attack themselves that may fall inside the remit of the jus ad bellum to the degree that they amount to a use of force. In paper we will examine the use of the law of self-defence in the cyber discourse. It will be seen that the lessons (exmples) learned corresponding to global terrorism are valuable for making a legitimate worldview for self-defence against cyber attacks.

Keywords: self-defence, cyber attacks, international humanitarian law, jus ad bellum

Introduction

Article 51 of the UN Charter says "Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council (SC) has taken measures necessary to maintain international peace and security".[1] The state that became the victim of the cyber attack can so be entitled to respond in self-defence only to the extent where the use of such an attack can be characterized as an armed attack. In the Nicaragua case, the ICJ acknowledged that a definition of an "armed attack" does not exist in the UN Charter. The ICJ, nevertheless, made

[1] UN Charter, Art 51.

it clear that Article 51, does not refer to any peculiar weapons and that it applies to any use of force in spite of the weapon utilized.[2] Similarly, the various exceptions pose that the Article 2(4) provides a blanket protection for the prevention on that of the use or threat of force which consists of two exceptions such as the actions which are taken as any part of that of the collective security operations and the other is considered to be the actions which have been taken in self defence.[3] The first exception is considered to fall under that of Article 39 of the Charter of UN. It authorizes the Security Council to regulate and determine any kind of existence related to threat to peace or any breach related to peace or any act relating to aggression. It also provides with making some kind of recommendations or decide some kind of measures, which can be taken in order to maintain and to restore any peace or security in the international arena. The Security Council is considered to employ measures which would not involve any kind of armed force and authorize any actions which would be by any, land, air or sea.[4] These collective security operations under that of the Article 39 is considered to be politically difficult as they require some kind of authorization. Moreover, these are considered to be easily recognizable and such are also uncontroversial. If there has been any kind of authorization by the Security Council then the use of force which would be in retaliation to such would be considered to be in the form of cyber attack and therefore, a state's actions would be considered to be lawful and the actions would likely be considered to be within the scope of that specific authorization.

The second exception to the Article 2(4) would be articulated within Article 51 as such provides that nothing which is considered to be contained in the UN Charter would be able to impair the inherent right of that of the individual or any collective self defence if any kind of armed attack takes place.[5]

The self defence which is considered to be lawful is considered to be difficult to recognize than that of the operations of that of the lawful collective security. If there has been any kind of armed conflicts there is a possibility that both the states involved in such would claim for acting in self defence and such debates regarding international law focuses more on the factual and other political disputes rather than that of the legal doctrine. Cyber attacks would constitute as self defence for armed attacks only through three kinds of approaches regarding the instrument based approach, the effects based approach and the target based approach.

According to the Article 51 the cyber attack is not considered to be an armed attack as such lacks the physical characteristics which are considered to be

---

[2] Roscini, Marco, "World Wide Warfare- jus ad bellum and the use of cyber force", *Max Planck Year book of United Nations Laws* , vol, 14, (2010), Pp 85-130

[3] UN Charter Art 2(4)

[4] UN Charter Art 39.

[5] UN Charter Art 51

traditionally associated with that of the military coercion as such does not have any traditional weapons and the instrument based approach would only consider the traditional weapons to be used for an armed attack. The target based approach is considered to permit and allow the aggressive protection for any kind of critical national systems which would broadly sanction the forceful self defence which would increase the likelihood of the cyber conflicts and be able to intensify into more destructive armed conflicts which would be conventional.[6] These attacks are considered to penetrate into a crucial system which would justify the military response in a conventional way that would be able to start some kind of a physical war. Such an approach is considered to harm the security of that of the international community by making the war much more probable.

Thirdly, the effect based approach is considered to provide the cyber attacks and compare it with the armed attacks only based on the gravity of such.[7] The effect based approach is considered to measure the gravity through various factors from that of the sheer severity of the harm which has been caused due to the length of the effect of the cyber attack and the harm which has been caused. Such also provides with a common orientation with that towards the inquiry.[8]

Collective self-defence in reaction to a cyber armed attack

Article 51 considers individual as well as collective self-defence, in this case, the state utilizing defensive force responds against an armed attack that targeted another state. collective self-defence against digital armed attacks has been integrated in Rule 16 of the Tallinn Manual.[9] Collective self-defence is subjected to similar conditions as individual self-defence, like, the happening of an armed attack, and the necessity, proportionality, and immediacy of the response, whose

---

[6] Barrett, Edward. "On The Relationship Between The Ethics And The Law Of War: (Cyber Operations And Sublethal Harm)*", Ethics & International Affairs 31, no. 4* (2017),Pp.467-477. doi:10.1017/s0892679417000454.

[7] McKibben, Heather Elko. "To Link Or Not To Link? Changing The Bargaining Structure With An Issue Linkage Strategy". *SSRN Electronic Journal*,(2012). doi:10.2139/ssrn.2142202.

[8] Czosseck, Christian, Rain Ottis, and Anna-Maria Talihärm. "Estonia After The 2007 Cyber Attacks". *International Journal Of Cyber Warfare And Terrorism* 1, no. 1 (2011),Pp.24-34. doi:10.4018/ijcwt.2011010103

[9] Tallinn Manual, p 67

application in the digital perspective and ambit has effectively been analyzed and discussed in the study already.

Additionally, as explained by the ICJ in the Nicaragua judgment, collective self-defence likewise necessitates that the victim/suffered state announces itself to be the victim of an armed attack and demands help to repulse it.[10] One mode of exercising collective self-defence is through a military coalition set up for that particular purpose.[11] The primary international organization or association for the collective self-defence today is NATO.

The Organization espoused a digital defence strategy/policy in 2008, which was re-examined/amended in June 2011 along with the adoption of a related Action Plan for its implementation. NATO has likewise made a Cyber Defence Management Authority, a Computer Incidence Response Capability and the Cooperative Cyber Defence Center of Excellence (CCDCOE). The Organization has led digital defence exercises/practices with the cooperation of groups from member states and marked memoranda of understanding (MoU) in relation to cyber security with some member states, including Estonia, Slovakia, Turkey, the United Kingdom, and the United States.[12]

The primary question in the NATO perspective is whether digital activities against member states should fall under Article 4 of the NATO Treaty, which stipulates for an obligation to consult whatsoever point, in the appraisal and opinion of any of them, the regional integrity, political autonomy or security of any of the Parties is compromised, or Article 5.[13] Article 5(1) provides that;

---

[10] Nicaragua, para 199.

[11] Dinstein, "War, Aggression and Self-Defence",*Cambridge University Press*, 5th edn, pp 286–9

[12] Hamadoun I Touré, "The International Response to Cyberwar", in *The Quest for Cyber Peace*, edited by Hamadoun I Touré et al, ITU, January 2011, p 103

[13] Article 5 has been invoked only once in NATO's history in response to the 11 September 2011 attacks against the United States. Article 4 has been formally used in February 2003, when Turkey requested consultations on the effects of the impending Operation Iraqi Freedom on its security (Ulf Häussler, "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty", in *International Cyber Security Legal and Policy Proceedings*, edited by Eneken Tikk and Anna-Maria Talihärm (Tallinn: CCDCOE, 2010), p 103

"the Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area".[14]

It is to be reviewed that there is no automatism in the collective response to an armed assault and that NATO states have consistently reasoned that the decision of what assistance to give/provide was eventually theirs.[15]The question is whether the casus fœderis ("case for the alliance") as an "armed attack" against at least one of the members additionally includes digital attacks. It is important to note that Estonia a NATO member state, was the target of a DDoS attacks in 2007. Despite the fact that Article 4 was not officially call forth, it appears to be that consultations occurred after the attacks[16], while the Estonian Defence Minister was said to consider about conjuring of Article 5.[17]

During that emergency situation, notwithstanding, the Minister asserted that "NATO doesn't characterize digital attacks as a clear military activity/action. This

[14] Also see Art 3(1) of the Rio Treaty. Unusually, the 2005 AU Non-aggression and Common Defence Pact employs the broader notion of "aggression" instead of "armed attack" (Art 4(b)). The OAS has adopted a *Cyber Security Strategy* in 2004, which nevertheless focusing on cyber crime and cyber terrorism, and not on the military utilization of cyberspace by states.

[15] Häussler, Ulf. "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty". In *International Cyber Security Legal & Policy Proceedings*, edited by Eneken Tikk and Anna-Maria Talihärm (Tallinn: CCDCOE, 2010), p 120

[16] Häussler, Ulf. "Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty". In *International Cyber Security Legal & Policy Proceedings*, edited by Eneken Tikk and Anna-Maria Talihärm (Tallinn: CCDCOE, 2010), p 120

[17] Scott J Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law", *Berkeley Journal of International Law* 27 (2009), p 194.

implies that the provisions of Article 5, will not automatically be extended and that this matter necessarily be settled soon.[18]
It ought to be noticed that Article 5 of the NATO Treaty determines that, to actuate thecollective self-defence mechanism, the armed attack against one of the states parties should happen in Europe or North America. Article 6 further notes that a an armed attacks on at least one of the parties includes an armed attack;

- "on the territory of any of the Parties in Europe or North America, on the Algerian Departments of France, on the territory of or on the Islands under the jurisdiction of any of the Parties in the North Atlantic area north of the Tropic of Cancer",

- "on the forces, vessels, or aircraft of any of the Parties, when in or over these territories or any other area in Europe in which occupation forces of any of the Parties were stationed on the date when the Treaty entered into force or the Mediterranean Sea or the North Atlantic area north of the Tropic of Cancer".[19]

The way that digital assaults happen in and through the internet using cyberspace, and not in the particular territoriall arena demonstrated in Articles 5 and 6, doesn't prevent
that such attacks can possibly fall under the extent of those provisions. Indeed, as has been seen,[20] it is at where the cyber activities arise and where their consequences happen that one needs to take a gander at to "territorialize" them, hence, a digital activity that causes death or injuries to people, actual harm to property, or serious disturbance of the operation of basic infrastructure situated in Europe or North America would meet the geographical prerequisites of Articles 5 and 6.
Regardless, it is currently wel established that "coercive conduct" by NATO may take place even beyond the geographic limits of the European and Atlantic region

[18] Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia", *The Guardian*, 17 May 2007,

[19] Roscini, " Cyber Operations and the Use of force in International law", *Oxford University Press*, pp 95-97

[20] Roscini, " Cyber Operations and the Use of force in International law", *Oxford University Press,* pp 95-97

if practically connected to the need to react/respond to dangers that could imperil stability and security in the area".[21]

The duty to report the self-defence measures to the UN Security Council

Article 51 of the UN Charter requires states espousing measures in individual and collective self-defence to report them on instantly to the UN Security Council. Such a responsibility/duty may be hard to abide by on account of a digital attack in self-defence, it has been seen that, as a result of their intrinsic characteristic/attributes and the current design of the internet/cyberspace, cyber operations are the ideal instrument for incognito activities. Therefore, a question arises here from the above that, does it mean that a ditital attack in self-defence would not be lawful if it is not promptly brought before the Security council?

The question emerged in more broad terms in the Nicaragua case, as the US paramilitary activities in and against Nicaragua were carried out secretively i.e. (in a covert manner) through the CIA and agencies. The Court established that the obligation to report doesn't reflect customary international law (atleast that was not customary law at the time of the court's decision),[22] however that it may be one of the elements demonstrating whether the State in question was itself persuaded/confident that it was acting in self-defence.[23] Surely, a State can't be denied and can't deny itself, of its innate right of individual or collective self-defence as a result of its inability to report steps/meaures taken in the exercise of that right to the Security Council.[24]
Consequently, it can be inferred that the incognito nature and quality of defensive virtual activities does't as such render them unlawful under Article 51 of the UN Charter, giving that any remaining requirments to the exercise of self-defence are fulfilled/met. The inclusion of Rule 17 in the Tallinn Manual, according to which " measures involving cyber operations undertaken by States in the exercise of the right of self-defence pursuant to Article 51 of the United Nations Charter shall be immediately reported to the United Nations Security Council", seems, consequently, of restricted pragmatic importance and relevance.

Chapter VII of the UN Charter and the Role of the Security Council

Despite its characterized as an armed attack, the state suffered/victim of a digital activity could allude the circumstance/situation to the Security Council under

[21] Enzo Cannizzaro, "NATO's New Strategic Concept and the Evolving Legal Regulation of the Use of Force", *The International Spectator* 36, no 1 (2001), p 70.

[22] Gray, International Law, pp 101–2, and Nicaragua, para 200

[23] Nicaragua, para 200

[24] Nicaragua, Dissenting Opinion of Judge Schwebel, para 230

Article 35(1) of the UN Charter and the Council may commend/prescribe the fitting techniques/methods to settle the issue/dispute (Article 36(1)).

Whenever that the Security Council additionally demonstrates/bases that the circumstance adds up to a danger to the peace and harmony, breac of peace, or act of agression (animosity), it could exert its powers and authority under Chapter VII of the UN charter. The exertion of this ability/competence by the Council likewise establishes a limit to the right of individual and collective self-defence by states, as given in Article 51 of the UN Charter.[25]

Regardless of whether digital tasks can be viewed as penetration of the peace & harmony or acts of aggression(animosity) (Article 3(b) of GA Res 3314 (XXIX), for example, determines that "the utilization of any weapons by a State against the territory of another State may add up/amount to an act of aggression), they could surely conceivably/possibly add up to a danger to the peace and harmony". The creators/source (staes or non-state actors) of the digital activity, just as its portrayal as a utilization of force, armed attack, or simple digital misuse, would not be a definitive factor in the determination that a danger to the peace & harmony exists. Thus, despite the fact that, in the drafters persuation, this idea was restricted to the international use of armed force,[26] its extension has been dynamically extended by the Security Council.[27]
The General Assembly has over and over again communicated/declared its concern that digital technologies can conceivably be utilized for purposes that are in voilation or inconsistent with the objectives of keeping international stability and security.[28] Cuba has emphasized that the abuse of data systems and

[25] According to Art 51, the right of self-defence exists "until the Security Council has taken measures necessary to maintain international peace and security". It appears, nevertheless, that the Security Council necessarily to indicate an unequivocal intent or purpose to terminate the right of self-defence of the victim and other states for this limitation to apply (Gill and Ducheine, "Anticipatory Self-Defense", pp 447–8)

[26] Inger Österdahl, Threat to Peace. The Interpretation by the Security Council of Article 39 of the UN Charter (*Uppsala: Iustus, 1998*), p 85

[27] It is known that the authors of the Charter intentionally left the concept vague (United Nations Conference on International Organization, Documents, Vol XII, 1945, p 505)

[28] Preamble, GA Res 66/24, 2 December 2011.

resources for meddling in the internal issues of different states and encroaching their sovereignty and independence what's more, autonomy may represent a genuine danger to worldwide security.[29]

The US International Strategy for Cyberspace also notes that "cybersecurity threats can even endanger international peace and security more broadly, as traditional forms of conflict are extended into cyberspace".[30] "Bolivia, China, Estonia, Mexico, Panama, Poland, Russia, Sweden on behalf of the EU member states of the United Nations, and Turkmenistan"[31] have all declared analogous concerns. Article 4 of the draft Convention on Information Security intended by Russia, in particular, lists of risks and threats in the information space detrimental to "international peace and stability":

1) "the use of information technology and means of storing and transferring information to engage in hostile activity and acts of aggression";

2) "purposefully destructive behavior in the information space aimed against critically important structures of the government of another State";

3) "the illegal use of the information resources of another government without the permission of that government, in the information space where those resources are located";

4) "actions in the information space aimed at undermining the political, economic, and social system of another government, and psychological campaigns carried out against the population of a State with the intent of destabilizing society";

5) "the use of the international information space by governmental and non-governmental structures, organizations, groups, and individuals for terrorist, extremist, or other criminal purposes";

6) "the dissemination of information across national borders, in a manner counter to the principles and norms of international law, as well as the national legislation of the government involved";

7) "the use of an information infrastructure to disseminate information intended to inflame national, ethnic, or religious conflict, racist and xenophobic written

[29] UN Doc A/54/213, 10 August 1999, pp 4–5

[30] International Strategy for Cyberspace, p 4.

[31] UN Doc A/58/373, 17 September 2003, p 2., UN Doc A/59/116, 23 June 2004, p 4, Estonia's Cyber Security Strategy, p 10, UN Doc A/59/116/Add.1, 28 December 2004, p 2, UN Doc A/57/166/Add.1, 29 August 2002, p 5, UN Doc A/55/140/Add.1, 3 October 2000, p 2, UN Doc A/C.1/65/PV.15, 20 October 2010, p 20, UN Doc A/56/164, 3 July 2001, p 5, UN Doc A/66/152/Add.1, 16 September 2011, p 7

materials, images or any other type of presenting ideas or theories that promote, enable, or incite hatred, discrimination, or violence against any individual or group, if the supporting reasons are based on race, skin color, national or ethnic origin, or religion";

8) "the manipulation of the flow of information in the information space of other governments, disinformation or the concealment of information with the goal of adversely affecting the psychological or spiritual state of society, or eroding traditional cultural, moral, ethical, and aesthetic values";
9) "the use, carried out in the information space, of information and communication technology and means to the detriment of fundamental human rights and freedoms";

10) the denial of access to new information and communication technologies, the creation of a state of technological dependence in the sphere of informatization, to the detriment of another State";

11) "information expansion, gaining control over the national information resources of another State".[32]

The issue, be that as it may, is whether any digital activity, whatever its nature, proportion, and outcomes, can be qualified by the Security Council as a danger to the the peace and harmony in the purview of Article 39 of the Charter. Despite the fact that the Council enjoys a wide discretion in deciding and determining the existing of such a threat, this competence isn't unlimited, a danger to the harmony couldn't be artiicially made as an appearance/guise for the recognition of ulterior purposes.[33]

The ICTY clarified that "the danger to the harmony" is to a greater extent a political idea. Yet, the determination that there exists such a danger is anything but an absolutely unchained discretion, as it needs to stay, in any event, within the restrictions of the Purposes and Principles of the Charter[34], According to Conforti, "the conduct of a state cannot be considered a threat to the peace when

[32] Draft Convention on International Information Security (Concept), 2011, Art 4.

[33] Legal Consequences for States of the Continued Presence of South Africa in Namibia (South West Africa) nevertheless Security Council Resolution 276 (1970), Advisory Opinion, 21 June 1971, ICJ Reports 1971, Dissenting Opinion of Judge Fitzmaurice, paras 116–17.

[34] *Prosecutor v Tadić*, Case No IT–94–1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, para 29

the condemnation is not shared by the opinion of most of the States and their peoples".[35]

Different scholarly persons allude to the limit of good faith and to the philosophy of exploitation of right.[36] Undoubtedly there is no immediate judicial control over actions of the Council[37], however there are aberrant or indirect ones, the dissent or objection by refusal to abide by the resolution by the UN member states, the aberrant/indirect legal control when a resolution gets pertinent to decide a case before a international or domestic court or tribunal, and, all the more by and large, acknowledgment of the Security Council's act by the international community.[38] In order to establish the presence of a danger to the peace and harmony, at that point, the position of the penetrated standard (norm) or worth,

[35] Benedetto Conforti, "The Law and Practice of the United Nations", 3rd edn (*Leiden and Boston: Nijhoff*, 2005), pp 176–7

[36] Thomas M Franck, "Fairness in the International Legal and Institutional System", *Recueil des cours* 240 (1993–III), p 191

[37] In his Separate Opinion in the *Genocide* case, Judge ad hoc Lauterpacht recalled that the ICJ's power of judicial review 'does not embrace any right of the Court to substitute its [own] discretion for that of the Security Council in determining the existence of a threat to the peace, a breach of the peace or an act of aggression, or the political steps to be taken following such a determination' (*Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro),*

[38] Michael Bothe, "Les limites des pouvoirs du Conseil de sécurité", in *The Development of the Role of the Security Council—Workshop of the Hague Academy of International Law*, edited by René-Jean Dupuy (Dordrecht: Nijhoff, 1992), p 70

the seriousness of the infringement, and its transboundary impacts should be contemplated.[39]

The appraisal would clearly rely upon the particular circumstances of each case. For example, as the US Department of Defence stresses, "a computer network attack caused widespread damage, economic disruption, and loss of life could well precipitate action by the Security Council".[40] Another likely illustration of danger to the peace and harmony in the digital context is "any genuine virtual attack by competiters in long-standing worldwide blaze points, like India–Pakistan and Turkey–Greece)".[41] Iran has likewise supported the Security Council "to act against those States undertaking digital assaults and harm in the peaceful atomic facilities".[42] On the other hand, it has been proposed that "Computer assaults among significant Western economic powers. . .would obviously not compromise the peace and harmony if discovered".[43]

Whenever the Security Council does declare a cyber activities or operation as a menace to the peace and harmony, breach of the peace, or act of aggression, it could make recommendations under Article 39, follow measures intended at preventing the deterioration of the situation under Article 40, and, more importantly, adopt coercive measures under Articles 41 and 42. The non-exhaustive list of measures that the Council can recommend or decide under Article 41 includes "complete or partial interruption of. . .telegraphic, radio, and other means of communication": the Security Council could hence follow targeted cyber sanctions or limit the access to the internet of the state accountable for the menace to the peace, breach of the peace, or act of

---

[39] Opinion of judge ad hoc Lauterpacht recalled that the ICJ's power of judicial review "does not embrace any right of the Court to substitute its own discretion for that of the Security Council in determining the existence of a threat to the peace, a breach of the peace or an act of aggression, or the political steps to be taken following such a determination" (*Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro)*, Further Requests for the Indication of Provisional Measures, Order of 13 September 1993, ICJ Reports 1993, para 99).

[40] US Department of Defence, An Assessment, p 15.

[41] Micheal,Schmitt, "Computer Network Attack and the Use of Force", p 928

[42] Iranian Foreign Minister's address to the UN Security Council, 28 September 2012

[43] Micheal, Schmitt, "Computer Network Attack and the Use of Force", p 928.

aggression". Member states might be needed to forbid the provision to the targeted on state of hardware and programming that encourage association with the web and to guarantee that website pages are denied access from the domain name of the targeted state.[44]

The UN member states may likewise be needed to adopt enactment to execute the sactions in their municipal legal system, for example to condemn and criminalize certain digital activities and conduct or to require domestic Iinternet service provider (ISPs) to follow prohibitive measures.[45]

Should the Security Council consider that actions stipulated in Article 41 would be deficient (inadequate) or have end up being deficient (inadequate),[46] it could approve UN member states or UN peace forces to lead digital assaults adding up to a utilization of force to respond against a danger to the peace.[47] The reality of the matter is that Article 42 in particular alludes to enforcement action "by air, sea, or land forces" a exacting perusing of the provision may prompt to the that conclusion that enforcement in the cyberspace is obstructed or forestall to the Council.The intention of Article 42, nevertheless, was to extend the collective security machinery to all military sphere accessible at the time the Charter was drafted.[48]

Anticipatory self-defence against an imminent armed attack by cyber means

Article 51 states that "an armed attack must occur" in order to initiate or activate the right of self-defence by the victim. In Nicaragua case, the ICJ did not assumed a perspective on the question of self-defence against attacks that have as yet to happen, since "the issue of the legality of a response to the approaching menace of armed attack" was not raised.[49] Essentially, for the situation concerning Armed actions or activities in the region of the Congo the Court communicated

[44] UN Doc A/67/167, 23 July 2012, pp 10–11

[45] Tallinn Manual, p 70

[46] Article 42 of the UN Charter.

[47] Harrison Dinniss, "Keeping the Cyber Peace: International Legal Aspects of Cyber Activities in Peace Operations", *International Law Studies* 89 (2013), pp 523–7.

[48] Nills, Melzer, "Cyberwarfare and International Law", *UNIDIR*, 2011, p 19.

[49] *Nicaragua V. United Staes*, para 194

no view on this issue, as Uganda eventually and finally asserted that its activities were in light of armed attacks that had effectively happened.[50]

The Court, in any case, cognizant that the security needs that Uganda expected to defend and protect were basically preventative[51] and held that Article 51 of the Charter may legitimize a utilization of use in self-defence only within the stern limits there set down. It doesn't permit the utilization of force by a State to defend and protect perceived security interests beyond these boundaries.[52]

Dinstein employs the notion of "interceptive self-defence to indicate a reaction to an event that has already begun to happen even if it has not yet fully developed in its consequences[53] and maintains that, in such case, self-defence can be invoked under Article 51 because an armed attack 'is already in progress, even if it is still nascent".[54]

Others allude to the advent of the armed attack to recognize anticipatory and pre-emptive responses. The latter, which alludes to nascent attacks that may or may not emerge at some indistinct point later on, is for the most part thought to be conflicting with international law, not just does it run against the letter of

[50] Armed Activities on the Territory of the Congo (DEMOCRATIC REPUBLIC OF THE CONGO) *DRC v Uganda*, para 143, Judgment, 19 December 2005, ICJ Reports 2005.

[51] *DRC v Uganda*, para 143

[52] *DRC v Uganda*, para 148

[53] Yoram Dinstein, War, Aggression and Self-Defence, 5th edn *(Cambridge: Cambridge University*

Press, 2011), p 203

[54] Dinstein, "War, Aggression and Self-Defence", *Cambridge University Press*, 5rd edn pp 204–5.

Article 51 of the UN Charter yet it is additionally not upheld by broad and uniform state practice and opinio juris.[55]

Preemptive self-defenec is similarly at likelihood with the prerequisites of necessity and proportionality that any self-defence response should agree with, the further on schedule and the more dubious the attack, the less vital the defenssive armed response is, and the more troublesome the figuring of its proportionality. Then again, a right of anticipatory self-defence against an unavoidable imminent armed attack is consistent not only with customary international law as well as with Article 51 UN Charter.[56]

The facts demonstrate that, under actual reading of this provision, the armed attack must happen, at the same time, as per Article 32 of the 1969 Vienna Convention on the Law of Treaties, the use of the Article 31 interpretive criteria ought not tend to a rendition which is obviously ludicrous or preposterous. The reationale or reasoning of self-defence is to empower the victim to deflect an armed attack, if the risk is exigent, overpowering, leaving no choice of means, and no second for consideration.

Anticipatory self-defence against approaching cyber armed attacks has been integrated in Rule 15 of the Tallinn Manual.[57] Anticipatory self-defence against a cyber attack that preludes an approaching active armed attack, as on account of Israel's Operation Orchard against a Syrian atomic facility, or anticipatory self-defence by digital means against an unavoidable kinetic armed would not make issues fundamentally unique in relation to those previously emerging in a

[55] Antonio, Cassese, International Law (*Oxford: Oxford University Press*, *2005*), p 361; "Gray, International Law, pp 213–16. The doctrine of pre-emptive self-defence was elaborated in the 2002 US National Security Strategy (reaffirmed in 2006), that tried to expand the definition of "imminence" of armed attack well beyond the Caroline requirements to cover cases where 'uncertainty remains as to the time and place of the enemy's attack' (The National Security Strategy of the United States of America, 20 September 2002, p 15,

[56] A UN Report, "A More Secure World", para 188; In Larger Freedom: Towards Development, Security and Human Rights for All, Report of the UN Secretary-General, UN Doc A/59/2005, 21 March 2005, p 33

[57] Tallinn Manual, p 63

conventional situation.[58] It is safe to contend that, if, just before the 1967 Six Days War, Israel had responded to the massing of troops at its boundary by its Arab neighbors and to the obstruction of the Strait of Tiran not by besieging (bombarment) the Egyptian air force on the ground before the airplane could take off and deliver the attack on the Jewish state, yet by weakening Egypt's air force radars and order & control systems with a monstrous digital (cyber) attack, the lawfulness of such attack would have most likely not been questioned.

Without a related dynamic assault (attack), in any case, anticipatory self-defence by digital or dynamic (kinetic) methods against an inescapable or appraoching independent digital armed attack will be exceedingly hard to bring up or evoke in practice, in the deficit of noticeable indications,convincingly building up the source point, nature, and advent of the digital attack and the need and proportionality of the response may end up being an outlandish and unattainable task.[59]

In fact and surely, as will be ascertained, that states asserting and demanding a right of anticipatory self-defence will have to render, atleast a minimal, apparent and convincing' grounds and prrof of the imminent attack. In the present circumstance, at that point, the decision is between keeping the imminence necessity and requirment in its literal temporal understanding or meaning so the interfering state's edge of appreciation is restricted and mishandles are exorcized however at the expense of limiting the defensive option or alternative of the suffered state, or decide and prefer on more adaptable sensibility guidelines that consider the particular highlights of digita (cyber)l operations and the nature and extent of the danger.[60]

While states that seek after assertive and forceful policies or on the other way around, states that are the regular prey or objective of cyber attacks, are probably going to support the more adaptable way to deal with imminence, states that don't assume an active role in the digital field and dread potential maltreatments by more impressive states will most likely go for the stricter transient idea of imminence.

Conclusion

[58] Terry D Gill and Paul AL Ducheine, "Anticipatory Self-Defense in the Cyber Context", *International Law Studies* 89 (2013), p 465

[59] Gill and Ducheine, 'Anticipatory Self-Defense', p 466, and Matthew C Waxman, 'Regulating Resort to Force: Form and Substance of the UN Charter Regime', *European Journal of International Law* 24 (2013), p 160.

[60] Matthew C Waxman, "Regulating Resort to Force: Form and Substance of the UN Charter Regime", *European Journal of International Law* 24 (2013), p 160-1

As we know that the present rules of jus ad bellum do not offer any direct rules applicable to cyber operations or cyber activiteis. It is said that the current rules of jus ad bellum are flexible and, therefore can be extended to cyber activities, this analogy shows that the current rules are not sufficient to be applied directly to such operations and hence, were not existent when they were adopted. Entirely, it is the states themselves that have contended that the current and existing rules of jus ad bellum can be made applicable to at least certain cyber activities or cyber operations.

A cyber attack or cyber operation which is carried out by one state against another state and which causes and possibly to cause destruction in the form of material damage to property, loss of life or bodily injury to individuals and extreme disruption of basic funtions of the critical infrastrutures of the victim state, is hence prohibited by the Article 2(4) of the UN charter. A cyber attack of such nature will be governed by Article 2(4) of the UN charter and is therefore considered to be a use of force against a state. Similarly, those cyber attacks or activities which do not cause destruction of a material damage to property or loss of life or bodily injury to individuals may not amount to the use of force under Article 2(4) and will be considered wrongful or illegal interference or interventions in the domestic affairs of other state.

Likewise, those cyber activities which are carried out by one state against another and do not reach to the threshold of use of force are considered to be interferences and voilation of another state's soveriegnty. Such cyber activities are never a use of force under Article 2(4) of UN charter. The right of self defence under Article 51 of the UN charter may be exercised in case of a cyber attack carried out by a state or a non-state actors, only when it amounts to the threshold of an armed attack. Self-defence against cyber attacks or operations do not reach to the threshold of an armed attack can be exercised entirely within the limits of the philosophy of the assemblage of events and of anticipatory self-defence.

In conclusion, the standard of evidence for right of self-defence against cyber attacks or operations amounting to an armed attack does not differ from that applicable to self-defence against actual armed attacks and would usually require clear and convincing evidence.