Journal of Politics and Law; Vol. 10, No. 4; 2017
ISSN 1913-9047 E-ISSN 1913-9055
Published by Canadian Center of Science and Education

Cyber Warfare and Self - Defense from the Perspective of International Law

Nazanin Baradaran[1] & Homayoun Habibi[2]

[1] PhD student in Public International Law, Department of Public and International Law, Faculty of Law and Politics, Science and Research Branch, Islamic Azad University, Tehran, Iran

[2] Assistant Professor, Department of Public and International Law, Faculty of Law and Politics, Allameh Tabatabai University, Tehran, Iran

Correspondence: Homayoun Habibi, Assistant Professor, Department of Public and International Law, Faculty of Law and Politics, Allameh Tabatabai University, Tehran, Iran. E-mail: homayounhabibi@gmail.com

Received: July 3, 2016 Accepted: August 14, 2016 Online Published: August 30, 2017

doi:10.5539/jpl.v10n4p40 URL: https://doi.org/10.5539/jpl.v10n4p40

Abstract

Cyber warfare represents new kinds of weapons in the present era that have the potential to change the battlefields. The different nature of these types of weapons and their ability to create massive and widespread damage to critical infrastructure of a state, subject the traditional means of resort to force to change and is indicative of the importance that the international community must come to some consensus on the meaning of cyber warfare with in the existing jus ad bellum paradigm and legislate its governing rules, On the other hand, the inherent rights of victim states in self-defense must be supported and by detailed explanations of the governing rules for the method of attribution of responsibility to governments committing cyber-attacks, actions must be taken to prevent escape of these governments from the consequences of their illegal actions. In fact, in this article with an analytical method we will examine the issue of whether cyber attacks could be considered as an armed attack trigger the right to self defense for victim states.

Keywords: use of force, cyber warfare, armed attack, self-defense, attribution

1. Introduction

The principle of non-resort to force as one of the most important principles of the United Nations Charter is: Article 2, paragraph 4, which in this article, it is only considered military force and the propounded prohibition in it is not only included its use, but also is included the threat of use of it., including the principle of the prohibition of the use of force is accompanied by some exceptions that is created by customary international law, the UN Charter and procedures have been followed. Besides the chapter VII resolutions in the Security Council, self-defense is the second exception acting on the principle of non-use of force that is stipulated to it in article 51 of the Charter.

The United Nations Charter is the result of discourse over rights in over sixty years. So what is propounded in paragraph 4 of Article 2 of the Charter as proposed banning the use of military force is the use of force by the classic and known weapons. But today, war has been taken away from its traditional concept in which weapons and explosives are used, and the improvement of technology has provided new tools for governments, which include most notably the use of cyberspace to carry out cyber-attacks against government targets. In fact, today the cyberspace is becoming a new field for tracking military operations, and as military experts have acknowledged, cyberspace is emerging as a new domain of war. This is while the major powers are equipping their forces faster and more extensively for cyber warfare, and actively benefit from it against their enemies and competitors. Generally, the cyber-attacks have a power that causes many destructive effects. For instance, cyber-attacks could disable a government's installations and civilian infrastructure such as power grids, railway, oil pipelines, airlines, transportation systems, financial markets etc. and thus threaten the life of a state.

Also, in recent years, cases of cyber-attacks have been increasing and many governments have been the target of cyber-attacks. In contrast, some governments have been the main suspect in the attacks, for example, the U.S. has been the target of several cyber-attacks that are claimed to have been performed by China. Another famous case is attacking the Estonia in April 2007 that for three weeks, the country was the target of cyber-attacks,

which caused the failure of official government websites, TV stations, banks, and so on. Cyber-attacks in other countries, including England, Taiwan, South Korea, Kazakhstan, Swiss, and so on, also have been occurred. And also our country, Iran in 2010 targeted by U. S.'s cyber-attacks aimed at disrupting the nuclear program through the Stuxnet virus. Nowadays, because of the importance of the issue, The intelligence services of U. S. has officially claimed that, about 20 to 30 countries are forming special units for cyber warfare and also NATO Put cyber warfare as new priorities on its agenda. According to the above mentioned issues and importance of the subject of this issue in the field debate on the right to war (force) was raised is whether intended this new tools including use of cyberspace to conduct cyber-attacks also could be considered as the use of force, the subject of Article 2, paragraph 4, of the Charter, and for the victim government of an armed attack provides the right to legitimate self-defense, the subject of the Article 51? In this regard it should be noted that on the one hand Article 51 besides the necessary condition, only if the right to self-defense for the victim government was detected that use of force is reached to the threshold of an "armed attack". So identifying cyber-attacks as an armed attack is a legal issue that should be studied and investigated. On the other hand, if such attacks take the name of an armed attack on their own, this important issue finds projection capabilities that how such attacks according to the complicated technical characteristics will be attributable to states suspected of committing these attacks? In this article the aim is to put forth the analysis of cyber-attacks issue from the projected dimensions.

2. Cyber Attacks as the Use of Force in International Law

Any purpose or motivation to provoke a government to run a cyber-warfare, and regardless of its normative assessment by the international community, the important subject is answer to the question of whether such cyber-attacks, either invasive or defensive are considered as the illegal threat or use of force? And thus if violates the rules of international law in this field?[1]

To define cyber-warfare, international community must somehow reach consensus on the meaning of these activities under the Charter, particularly Article 2, paragraph 4, which regulates the use of force set and Article 51 that provides the right to self-defense.[2] Article 2 paragraph 4 of the Charter describes the original sentence on the use of force in international law.

This regulation states that "all members in their international relations have to refrain from the threat or use of force against the territorial integrity or political independence of any state or in any way contrary to the purposes of the Charter.[3]

With this framework, the question is what action is considered as the use of force? Charter clearly has announced that the offensive force is illegal, while the inherent right of a state to self-defense as individual and/or popular identifies in the article 51.[4]

Thus, if the action of a government is considered as the use of force, according to the conception which is stated in Article 2, paragraph 4, of the Charter, is illegal unless it is in order to implement right of a country within the framework of article 51 of the Charter for self-defense.

While the precise definition of what is the use of force, is not clear, but some factors are well established.[5] For example, attacks by conventional weapons is in the context of paragraph 4 of Article 2 of the Charter.[6] Moreover, cyber-attacks, which are used for the purpose of directly damage physical property or cause human damage or death, are reasonably classified as the use of force and are therefore subject to this ban. In contrast, despite of the developing government's efforts for the inclusion of economic pressures in the context of paragraph 4 of Article 2 of the Charter at the time of Charter codification, these are clearly disqualified from the inclusion of this concept. Thus, the analysis based on the context of the Charter in paragraph 4 of Article 2, and history of the adoption of this part of the Charter requires interpretations that disqualify economic and political pressures from the inclusion of this Article.

The potential of the implementation of paragraph 4 of Article 2 of the Charter in cyber warfare creates serious interpretation problems for the difference between force and coercion. Inclusion of all actions related to cyber

[1]. MN Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework (1999). Columbia Journal of Transnational Law, Vol. 37, 1998-99.p.900, Available at SSRN: http://ssrn.com/abstract=1603800.

[2]. DM Greekman, a Helpless America? An Examination of the Legal Options available to the United States in Response to Various Cyber-Attacks from China, 17 AM. U. INT'L L, REV.641, 2002, p. 679.

[3]. Article 2, paragraph 4, of the Charter of the United Nations.

[4]. Article 51 of the Charter of the United Nations.

[5]. J Barkham, Information Warfare and International Law on the Use of Force, Fall, 2001, 34 N.Y.U. J. Int'l L. & Pol. 57,p.70.

[6]. Schmitt, op. cit, p.904

warfare within the meaning of the use of force, requires a broad interpretation of paragraph 4 of Article 2 of the Charter. With such a broad definition of force, disqualifying the political and economic coercions and forces from the cycle of this concept is difficult. Because international law should distinguishes between cyber-attacks that cause physical injury, such as electronic offensive and blocking of political and economic pressure, such as economic sanctions, but may often have the same results. Difficulty is in classifying between the cyber-attacks that do not cause physical injuries or indirectly has such effects against the prohibition of the use of force[7].

In an effort to resolve the impasse this category, Michael Schmitt distinguishes between the political and economic pressure and force by 6 criteria: 1) intensity 2) the urgency of 3) causation 4) violation of 5) quantifying 6) acquired legitimacy[8]. Through this criteria, act in cyber warfare against other acts are evaluated to determine whether the results of these acts are more like as the effects of armed attack, or whether the measures should be removed from areas of armed attack. Schmitt technique implementation leads to this result that the nature of predictable and logical results of the measures, determines whether it acts like an armed attack or not. If the results are similar to the effects of an armed attack, the development of the concept of force to these measures is reasonable, otherwise a wrongful act according to international law is occurred, which should be resorted to the other provisions of international law other than the prohibition of the use of force[9].

2.1 Cyber Attacks as an Armed Attack

What distinguishes a cyber-attack from other activities, such as cyber-exploitation of the internet, is its harmful effects in which a cyber-attack makes inaccessible the target system or endanger the health of its activities. An important question that can be asked here is whether such effects alone to make the right of self-defense in the absence of human and material damage are enough? The conditions for self-defense under Article 51 of the Charter should be reminded for this problem. The cases in article 51 of the Charter and customary international law are stated about the self-defense. Both branches of law seems that agree upon this case that what creates the right to self-defense is an armed attack on them. Although there is not any definition about what constitutes an armed attack in the Charter, but, what is accepted is that a cyber-attack as the use of force is defined by its intensity and effects and not on the basis of used tool[10]. As the International Court of Justice explains, an armed attack is the most severe form of the use of force in terms of scale and its effects. As a result of a cyber-attack which causes fundamentally destruction and the loss of human lives or great material destructions could be considered as an armed attack and performs the right of self-defense. For example, when a cyber-attack is done on air traffic control systems or nuclear reactors and causes vast human and financial damages, it is considered as an armed- attack.

A complex question and another problem is that the attacks on the critical infrastructure of a state which cause basic destruction but did not cause the human or material damage, could be considered as an armed attack and to make the right of self-defense? The answer to this question requires that we say what is critical infrastructure? Although there is no universally accepted definition but most definitions are agreed these cases that some particular services such as security, food, water, transport, banking and finance, health, energy, and public and government services are considered as critical infrastructures.

National U. S. Act of 2001 defines critical infrastructure as: systems and assets, whether physical or spiritual, which are very crucial for U. S. and disability and destruction of such systems and assets, has weakening effect on security, national economic security, national public health and safety, or any combination of these cases.

As a result, we can say that a cyber-attack on critical infrastructure which paralyze the government departments or cause large-scale destruction in them, should be considered as an armed attack, even if it does not cause the material damage or death of human beings immediately. For example, an attack on the governmental financial system through altering or destroying information that causes the risk of the economic life of a state, should be considered as an armed attack and this is not due to material destruction, but, it is for this reason that these attacks causes that the purpose for which such state infrastructure becomes unable to reach the goals which have been created because of them. Therefore such attacks on them should be considered as armed attack.

As a result, neither attack to Estonia in 2007, nor attack to Georgia in 2008, which was mentioned in the

[7]. Ibid.p.913.

[8]. Ibid.p.915.

[9]. VM Antolin-Jenkins, Defining the Parameters of Cyber war Operations :Looking for Law in the Wrong Places?51Naval L.Rev.132, 2005, p.170.

[10]. Tsagourias, Nicholas, Cyber Attacks, Self Defense and the Problem of Attribution Journal of Conflict and Security Law,Oxford University Press,2012,Vol.17,No.2, pp.229-244,pp.230-233.

introduction, are not considered as armed attack. In 2007, following the orders of the Government of Estonia about moving a Soviet-era memorial, banking and government websites were directly targeted by a series of cyber-attacks that led to their failure[11]. The same happened in 2008 in Georgia where the government websites were encountered with a cyber-attack of (DDOS)[12]which was coincided with the advent of the war between Russia and Georgia in August of the same year. The attacks does not cause human killing or material damages and service interruption that took place by those attacks was controllable. The idea that the cessation of service, is not an armed attack was highlighted by the fact that in the case of Estonia Article 5 of the North Atlantic Treaty Organization (NATO) that stipulates the right to collective defense if a government member is attacked by a State Party[13].

In connection with the above issue, this question can be raised whether a cyber-attack on military infrastructure of a country is an armed attack? If such an attack causes extensive damages, it would have the necessary criteria for self-defense, and it is not necessary that these damages to be material or human losses, but disruption of governmental services widely that would cause weakening and debility of the government, also will be sufficient. For example, a cyber-attack that weakens command and control systems by government, can be considered as an armed attack because the government's decision-making system has disabled, furthermore in many cases, such an attack could be as the introduction to an explosive and kinetic attack, that in such a case will create the right of pre-emptive self-defense.

Therefore the detection of a certain cyber-attacks which constitute an armed attack is very important, because cyber-attacks are often multi-layered and in them, the destructive influence that occurs in the systems, the implementation of loading and production of the harmful effects, may be occurred in different time intervals. If an attack is defined by its damaging effects which includes also the weakening effects of the attack, the attack is available once that its harmful effects are fulfilled, regardless of when the system is penetrated or the load is performed. However, if a government becomes aware that its systems are damaged, it can adopt active or passive defensive cyber measures to neutralize threats. A government may also considers this influence in the systems as an introduction to a cyber-attack or an explosion, if the available information indicates that this attack is a part of a general attack.

2.2 Cyber warfare and Self-Defense Exception

According to the Charter, there are two exceptions to the ban on the use of force: UN Security Council action on the basis of article 42 and individual or collective self-defense under and article 51 of the Charter[14]. Lawyers are disagree on the status of customary international law that is related to the use of force in self-defense and the proper interpretation of article 51[15]. Article 51 of the Charter says: in the event of an armed attack against a member of the United Nations, until the Security Council take the necessary measures to maintain international peace and security, none of the provisions of the Charter of the inherent right of self-defense, whether individual or collective will not damage, members should report immediately measures which in acts of this right of self-defense to the Security Council. These measures in no way will effect on the authority and responsibility that the Security Council have according to this Charter and whereby take the necessary action for keeping and restoration of international peace and security and whenever deemed necessary.

The scope of article 51 represents a subject of difference of opinion and notable debate among international lawyers[16]. Some of the lawyers interpret article 51 precisely and say that a government does not have the right of self-defense but when an armed attack has done against the government[17]. According to this interpretation, a government has not the right of action when there is an expectation of a force attack[18]. But in contrast of it, there are a large number of states that espouses of a vision that is against the limiting view and say that in certain circumstances, force may occur sometime before taking place of an armed attack. Lawyers who supported the second view believe that article 51 reflect customary international law and prescribes a pre-emptive self-defense.

[11]. Tikk and others, op. cit, pp.14-33.

[12]. Distributed Denial of Service.

[13]. NATO Parliamentary Assembly, Annual Session 2009, Committee Report 173 DSCFC 09 E bis- NATO and Cyber Defence' http://www.nato-pa. int/default.asp? SHORTCUT=1782 (accessed 19 June 2012) paras. 58-61.

[14]. SM Condron, Getting it Right: Protecting American Critical Infrastructure in Cyberspace, 20 Har V.J.L. Tech.403, 413 (2007).

[15]. Ibid.

[16]. Barkham, op. cit, p.74.

[17]. Ibid. pp.74-75.

[18]. Condron, Sean M., op. cit, p.412.

As by the Secretary of State, Daniel Webster[19] in the case of Caroline is raised, this issue occurs when the "necessity of self-defense is instant and there is no other choice and there is no time to consult".

Based upon the right of self-defense model, the response of a government to an armed attack must have three characteristics that would qualify for self-defense: necessity, proportionality, and immediacy. For the existence of the state of necessity, a government must be able to attribute an attack to a specific source. Clarifies the intention behind the attack and concludes that it should use of force in response. The principle of proportionality requires that the force that is applied in response be commensurate with the original attack. Also, the urgency prevents of the reactions that take place long after the attack. By considering of the urgency as a benchmark, however, there is no need to take defensive action immediately following the armed attack[20].

2.2.1 Necessity and Proportionality

The use of force by a state in order to carry out their right of self-defense which is also subjected to cyber operations, must be necessary and proportionate, i.e. measures in self-defense must meet two criteria of necessity and proportionality. International Court of Justice, at first suggested these two criteria in the Nicaragua case and then in the case of oil platforms approved it again. Nuremberg court is also recognized this criterion. As stated in these decisions, these two criteria are reflective of customary international law in this field. It should be noted that the concept of necessity and proportionality is different with the concept of military necessity and the rule of proportionality in right to war.

Necessity requires that the use force is also included that cyber operations, to repel an immediate attack or to defeat an attack that is happening. This does not mean that it is necessary that the use of force to be the only response available against armed attack, but it is only necessary that non-violent action against the situation to be insufficient. Of course, may be military action is also accompanied by non-coercive measures such as diplomacy, economic sanctions and so on. The key point in the necessity analysis in the field of cyber-attacks is the presence or absence of alternative measures that do not reach to the threshold of "use of force". If passive cyber defensive measures (that are different from active defensive measures) such as firewalls to thwart reliably and completely by a cyber-attack are sufficient, other measures, either cyber or kinetic, and explosive are as an illegal use of force. Similarly, if active cyber operations that have not reached as the use of force are adequate to fend off a cyber-attack, cyber coercive measures or alternative blasting action as necessary criteria are blocked and not to be done. However, when measures that are considered as the restricted use of force are not capable of defeat a cyber-attack or to prevent future attacks lonely, cyber and kinetic operations are included as the use of force on the basis of permitted right of self-defense[21].

The necessity benchmark is judged from the view point of the victim government. The definition of necessity must be reasonable and rational in conditions accompanied it. For example, consider the case that the government A begin cyber operations against government B where the critical infrastructure of the state B has encountered with essential material damages and lead to the loss of human lives. Previous attempts for negotiation has failed. Government B begins cyber operations to defend itself, while without knowing of the government B, the government A has decided to stop its operations. This reality does not deprive the government B from the right of performing cyber operations for self-defense as using allowable cyber force[22].

The proportionality evaluates the issue that how much of force which includes also cyber force is permitted, when there is the necessity of defense. This criteria limits scale, domain, interval, and the intensity of defense reaction, but this criteria does not limit the reaction as the amount of used force in the attack, since the amount and level of the force which is necessary to repel the attack successfully, depends on the situation. More amount of force may be necessary or less amount of force may be sufficient, to repel attack which has been carried out and/or repel imminent attack.

In addition, there is no requirement that the defensive measure in terms of nature is such as measures that has formed the armed attack. So, use of cyber force may be used in response to an explosive and kinetic cyber-attack or vice versa[23].

The proportionality requirement should not be exaggerated, since the origin of the armed attack may not be

[19]. Daniel Webster.

[20]. TD Gill, the Temporal Dimension of Self-Defence: Anticipation, Pre- Emption, Prevention and Immediacy, IIJ. CONFLICT & SECURJTY L.361, 369 (2006).

[21]. Tallinn Manual on the International Law Applicable to Cyber Warfare," op. cit, Rule 14, paras.1-6. para.3.

[22]. Ibid, para.4.

[23]. Ibid, para.5.

vulnerable against cyber-attacks, thus, kinetic and explosion operations in attempt for dissuading the rapist country from the continuation of the attack, should not be prohibited, although it should be used in the correct scale for achieving goal[24].

2.2.2 Imminence and Immediacy

The right of using force in self-defense is created when the armed attack is taken place or it is imminent. Therefore, this right is a function of the urgency necessity. Article 51 of the United Nations Charter refers to a situation where an armed attack occurred. Clearly, this article covers events in which the effects of armed attack has taken foreign shape, and this is when the cyber-attack has caused harm and damage, or it is creating such effects. They also include situations in which a cyber-attack is the first step in the stream of an armed attack. For example, cyber operations that directly against the air forces of a government is carried out and prepare the scene of war for air involvement. In this regard, lawyers believe[25] that although Article 51 of the Charter does not specified preemptive defense measures against an attack, but, it is not necessary that a government waits for preparation of the enemy for attack, and it could defense of itself when an attack is also imminent, this situation is called preemptive self-defense[26]. This situation is based on the urgency standards, which in the nineteenth century has been stated by Secretary of State of U. S., Mr. Webster following the Caroline case and was mentioned previously, and it is repeated because of importance. He in correspondence with his British counterpart, Lord Ashburton, by considering invade of Great Britain to the territory of U. S. to attack the Canadian rebels during the Mackenzie insurgence, stated that the right of self-defense is used when the self-defense necessity must be urgent, such that there is not remained any other alternatives, and also there is not any chance for the negotiation.

Although that incident is not related to measures which are done for preemption of an attack (Because the discussed attacks were ongoing), Webster formula as a classic expression of time threshold for preemptive defense measures has reached to date, and after that event, Nuremberg Court also approved Caroline affair correspondence[27].

International profession group approved this perspective that is stated by some commentators which self-defense measures are allowed when an attack has been done in reality and preemptive defense is prohibited, but, a definition somehow different from the previous perspective says that self-defense measure against a new attack that has not reached to its purpose[28] is allowed, but, the speed of cyber operations usually prevents of placing them in this category.

There is a variety of perspectives about the preemptive defense[29]. One perspective is that, it is necessary that armed attack is launched, consequently imposes a temporary restriction on preemptive measures. Most of the international profession group reject this analysis. They adopted the standard perspective "the last practical window of opportunity"[30]. By this standard, a state may acts preemptive defense including cyber, or explosive or kinetic, when the attacker clearly launched an armed attack was committed, and if the victim state does not act, it will lose the opportunity for the effective self-defense. In other words, this state may acts the preemptive defense during the interval of its last opportunity window against the nearby attack. This window exhibit itself immediately before the discussed attack, or in some cases a long interval before occurring of the attack. The important issue is not nearby time of preemptive defense against a future armed attack, but, the important issue is that if it is unsuccessful in measure on that moment, it will lead to this which logically that state is not anymore capable of effective self-defense when the attack is started. Consider a situation that in which the information services of the state A receives information that the state B is launching a cyber-attack that will destroy the oil pipelines of the state A in two weeks. The attack includes performing change in the micro-controllers operation along oil pipelines in order to increase pressure in them which will lead to explosive cases. The information system has not any information about this that which part would be damaged specifically, consequently refuses

[24]. Ibid, para.6.

[25]. Ibid. Rule15. para.2.

[26]. DW Bowett, Self-Defence in International Law188—189 (1958). Bowett Finds Support for this in the Travaux of the Charter's drafting Committee. Id.at 182 (Quoting Report of the Rapporteur of committee I to commission I, 6.U.N.C.I.O.459 (Jun, 13, 1945).

[27]. Nuremburg Tribunal Judgment at 435.

[28]. Y Dinstein, War Aggression and Self Defence, (5th ed-2011). pp. 230, 204.

[29]. Bowett, op. cit.

[30]. See for example: MN Schmitt, cyber Operations in International Law: The Use of Force, Collective Security, Self-Defence, and Armed Conflicts, in National Research Council of the National Academies, Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for U.S. Policy 160(2010).

to cyber defense of micro-controllers.

However, they have some information about this point which the attack will be done in a specific place and time. The behavior of the state A that concludes which should self-defense because of necessity is justified and legal, and acts as preemptive self-defense, because its lesser use is in-sufficient. In the evaluation of such cases should differentiate between the preliminary measures and the measures which compose the first phase of an attack. For example, consider the case of introducing a logic bomb to the computer system. This measure will be considered as an urgent armed attack, if a certain condition becomes possible for its activities. These conditions such as placing marine mines along the shipping path in the sea of the territory of the targeted state. This situation is different from placing active destructive remote software. If the inventor of the attack wants only to obtain the capability for the beginning of an attack in the future, the urgency criteria is not reached yet, but, if the inventor of the attack decides to perform an armed-attack by using of that malware, the armed-attacks in the time which the victim state should act, because it does not lose the opportunity for effective defense, becomes urgent. Of course, it is usually difficult to distinguish this difference practically. Legality of any defense by the evaluation of the operation of the victim state in that position is assessed[31].

Preventive Strikes[32], which is done against a future attacker that is lacking of either tools or willing of doing an attack, is not considered as a preemptive self-defense. Therefore, this fact that a state which is clearly enemy, is able to cyber-attack, even destructive attacks, lonely does not allow to the potentially victim state that measures in order to defense by using force. The potentially victim state should logically concludes at first that the enemy state really has a serious decision for attack. To achieve this result, the response of the victim government is limited to non-coercive countermeasures and refer the matter to the Security Council. Of course, even if a state has the goal and the opportunity of performing an armed-attack against another state, the right of the victim state for adoption of defensive measures to the limit of use of force, until the time that un-successfulness in measure causes that the ability of the victim state for effective self-defense, when the attacks begin, fail clearly, is not reached to the mature level[33].

The urgency necessity[34] (which differs from Imminence necessity) differs a self-defense measure from retaliation. This points to the time interval that is coming after the implementation of war and the victim state in it may act self-defense logically. Factors such as the temporary nearby time between attack and response, the required time for the identification of the enemy, and the required time for preparing itself for response, are proposed in this field. Another related subject in this field is the quality of the evaluation of the time interval that in which, a situation of self-defense followed by the completion of an incident which has composed the basis of the right of self-defense is continued. For example, a cyber-armed-attack may be started in a wave of cyber operations against the victim state. The situation of self-defense is not gained necessarily by the end of that cyber operations, if logically realizes that the next cyber operations may be occurred in continuation, and the victim state may encounter with them as a "cyber campaign", and continues the measure in order to self-defense. However, if this realization is not logical, every type of using force, either explosive or cyber, it is worthy that is categorized only as retaliation. In the final analysis, the Immediacy necessity is assessed by factors such as logicality, and considering the general conditions at that time[35].

In some cases, the fact that a cyber-attack has happened may not appear for a while. This may be due to this that the injury or damage was not yet identified. Similarly, may be the attackers could not be identified until after the attack. The classic example for both cases is the use of a worm like Stuxnet. In such cases, the criterion of urgency was not yet achieved, unless the circumstances described above, have been created[36].

3. Attribution in Cyber-Attacks

A state for cyber operations that violate international norms and it is attributable to the state, has international responsibility. This norm is established according to customary international law about the responsibility of states, and it is also reflected in the Articles of the International Law Commission plan for the state's international responsibility.

It should also be noted that the rules of the law of war also contains the specific rules on state responsibility for

[31]. Tallinn Manual, op. cit, Rule 15, para.6.

[32]. Preventive Strikes.

[33]. Ibid. para.7.

[34]. Immediacy.

[35]. Ibid. para.9.

[36]. Ibid. para. 10

violations of these regulations, in particular, Article 3 of the Convention Fourth Hague (IV) and Article 91 of the Protocol Annex I predicted that about violation some specific rules of warfare, compensation must be paid.[37]

3.1 Attribution: Political and Technical Aspects

If a cyber-attack reaches to the threshold of an armed-attack, it could perform the right of self-defense for the targeted state, and in this case, what is important is that, the attack is attributable to the suspected government. Thus, the assignment is necessary, but its implementation for the attacks such as terrorist attacks, and also for the field of cyber-attacks is extremely difficult and complicated, because, the nature of cyber territory is different from the other battles. Three specific attributes of the cyberspace makes the assignment issue extremely difficult. The first case is anonymity in which the attackers could hide their identity, the second case is the probability of performing cyber-attacks in several stages, in which a few computers which are controlled by different persons under the competence of different countries, perform operations before implementation of the main attack, and the third case is the speed and short time which a cyber-attack is done in it[38]. Finally, what is problematic, is not only tracking of the attack and specifying its source, for example a computer, but, specifying the identity of the person who controls the computer, and more important than it is specifying the mastermind behind the attack, and more critical is that all of them are occurred precisely and scheduled[39]. For example the attack of DDOS against Estonia in 2007 includes a big network including 85000 stolen computers from about 178 countries[40] that made very difficult the final identification of computers operators and the masterminds behind these attacks.

Therefore, assignment in cyber-attacks is a complicated procedure, and it has technical, legal, and political aspects which an aspect is related to the other aspect. By considering the technical aspects of assignment, even though science is improved continuously, the specified methods of assigning are also in progress, which could track the machine that attacked, and specify its place, but, simultaneously anti-tracking methods are in progress that could hide the origin of the attack. Furthermore, certain systems such as (TOR)[41] which is used by the army, could anonymous them. As a result, although the technical documents could have good yield, but they are never precise, and in addition, they are not always able to identify the identity of the person who implemented the operation[42]. For this reason, in addition to technical investigations, intelligence and analysis of information are also necessary for detecting the attackers or for preparation of information about the amount of their abilities, and also their purpose and/or their relation with other states[43]. The other point which is important in cyber warfare and it is almost the central problem, is the assessment by the safety professionals of the goals of an international player with respect to the goals of the other player[44]. For this goal, the political atmosphere in which the attack has occurred, or who benefits from it must be considered.

From the discussions above, it could be understood that assignment is a collection of technical investigations with political and intelligence assessments, and however, leads to create questions about the availability and verification of documents which assessments have been done on the basis of them. With regard to the availability of documents is also usually difficult to be able to achieve documents that are related to the safety issues, or the documents which are also available, are not often complete.

In the Nicaragua affair, Court also identified this problem where announced: "The issue of … is not a legal procedure of assigning an action to a specific state …, but, the issue is the previous procedure which on its basis, the material identity of the committed contrary acts has been proven[45]". About the cyber-attack, the issue that by the speed of the attack, committed crime anonymity, the probability and possibility of tricks, and this truth that this issue may have jurisdiction in many countries, causes the collection of documents be impossible in practice, or encounters with many political or legal problems[46]. In the Strait of Corfu incident, the court identified the

[37]. Refer to: ICRC Customary IHI Study, Rule 149-150.

[38]. N Tsagourias, "Cyber Attacks, Self –Defence and the Problem of Attribution", Journal of Conflict & Security Law, Oxford University Press 2012, pp.229-244, p.233.

[39]. DD clark and S Landau ,Untangling Attribution, National Security Journal, Harvard Law School,2011, p.37.available at: http://harvardnsj.org/wp-content/uploads/2011/03/Vol.-2_Clark-Landau_Final-Version.pdf

[40]. Tikk and others, op.cit, pp.20,23.

[41]. The Onion Router.

[42]. W Earl Boebert, A Survey of Challenges in Attribution, Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for U.S. Policy (National Research Council), National Academies press, 2010, 151 ff. pp.43-48.

[43]. Ibid. pp.49-50.

[44]. WM Reisman and an Armstrong, the Past and Future of the Claim of Pre-emptive Self- Defence, (2006)100 AJIL, pp. 525,526.

[45]. Nicaragua Case (Nicaragua V USA) op. cit, para. 57.

[46]. In view of the cyber-attacks on Estonia see: Tikk and others, op. cit, pp.27-28.

problems in the collection of documents when a land is under control of another state, and for this purpose, the court "commented an open source for conclusion truth and evidence related to the situation[47]". The second problem is related to the precision of documents which International Rights have not determined any specific and certain standard in relation to the problems that include use of force or self-defense.

Only a general standard that might exist are claims against the government, which was accused of exceptionally serious crimes and in this case should exist certain evidence to prove. Similar standard to prove the assignment is used for such actions[48].

This standard is less strict[49]. It is also higher than "without any doubt', or "beyond a reasonable doubt", or "balance of evidence", or "balance of probabilities" criteria. In any case, if the evidence is based on information that is usually because of the confidential nature of such information is inadequate, access to the listed standards is very difficult.

If the procedure of the International Court of Justice that considered the criterion of confidential evidence has value, it is shown a serious lack of exploration. In the case of genocide in Bosnia, for example, like the case of the Strait of Corfu, Court did not request the representation of classified documents by the defendant. A defect in the proceedings was criticized by one of the judges because those documents could clarify the general questions about the purpose and the capability of assignment.

It is resulted from the above discussions that standards with regard to the availability and the precision of documents in the affairs which are related to armed-attacks, use of force or involvement are proportionally inconsiderately, and in the affairs related to cyber-attack for the reason of mentioned characteristics is more such as this. Even if there is not proving standard such as that which is needed for the prosecution of persons, and even if one political approach in relation to assignment might accept less precise standards. This must be emphasized that a state should not resort to self-defense according to non-serious documents or political unreasonable inferences.

3.2 International Law Criteria on Attribution

With respect to the articles which were mentioned in the previous parts, if a cyber-attack combining with technical research and political analysis be attributed to a government, the victim government could act legally in self-defense against the aggressive government, if the criteria of international law concerning the assignment to make the right of self-defense is reached. Among the rules of international law and the International procedures, three important standards about the assignment are identifiable: According to the first criterion: attacks by organs of state are attributable to the state, according to the second criterion: attacks by the government agents trained by state has been directed or controlled by the government is also attributable to the state and based on the third criteria: the attacks that are tolerated the by the government are also attributable to the government. In all of the above examples, acting in self-defense could be done against the government involved in the attack. If none of the above cases cannot be applied, but a non-governmental player attacks to the other government, that non-governmental player will be the direct target of self-defense.

3.2.1 State Organs

On the basis of the first criteria, the operation of the organs of state is assignable to that state. Therefore, if an official and legal organ of a state, for example one of members of its army forces committed to a cyber-attack, that attack is attributable to that state which it will be the legal goal of self-defense for that state[50].

This assignment criteria is established based on the legal status of committing assault, and its reliability in some situations is recognized. For example, in the case of Nicaragua, the International Court of Justice, assigned the operation of the organs of U. S. to the state, while in the case of genocide in Bosnia, the Court examined the question whether the attempted genocide that occurred in Srebrenica is attributed to the Serbs as legal organs of the government of Serbia, but it was returned with a negative answer, because the persons that had done those crimes were not under the Serbian organs according to domestic law of Serbia[51].

[47]. Corfu Channel (United Kingdom V. Albania) (Merits) [1949] [ICJ] Rep 9, para.18 (Corfu Channel Case).

[48]. In other cases of the court used definitive or sufficient standard. See: Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo V Uganda) [2005] [ICJ] Rep 168, paras. 91 and 172 (Congo V Uganda).

[49]. The International Court of Justice also has mentioned standard without any doubt. Refer to: Bosnia Genocide Case, op. cit., para. 422; and, 'No Room for Reasonable Doubt Standard' see Corfu Channel Case, op. cit., para.18.

[50]. Bosnia Genocide Case, op.cit., paras. 385-95.

[51]. Nicaragua Case, op.cit., para. 109; Bosnia Genocide Case, Ibid,paras. 390-91, 307.

In addition to the organs' codes of conduct, the actions of operational organs in the government are also related to the government[52]. An operational organ is an institution which is absorbed in the state apparatus. Divan had this point in mind when stating in the Nicaragua Case that there should be a relation of complete dependence and control. The kind of control that the government should implement on such an institution should be in such a way that the institution treated as a operational organ in the government. This type of control covers all the activities of this institution. The international procedure regarding the degree of necessity of control in relation to the subordinate institution is not very accurate. For example, the Court speaks of an "effective control" criterion as well as "overall control" in the Nicaragua case; while in the case of the genocide in Bosnia, it requires a "strict control" criterion, or "a great degree of control". However, if these institutions act independently from the government in some ways, they could not be considered as the government's operational organs and therefore, their behavior will not be assigned to the government. In the Nicaragua case, for example, the Court did not assign the application of control to The United States, because it wasn't persuaded that the controlling was thoroughly related to The United States and acted as their operational organ. The Court made a similar conclusion about the case in Bosnia.

3.2.2 State Agents

The second standard regards an agency relationship where an institution acts under a government's instructions, direction or control. Therefore, a cyber-attack taking place by an institution that acts under the instructions of a state organ will be assigned to that state. These instructions create a temporary relationship between the state and the institution committing the attack; therefore, it should be proven that the instructions have been clear about the cyber-attack. The same argument is true about being under the state's directions. For instance, in the case of hostages of the U.S. Embassy in Tehran, the Court notes that in order to be able to assign the U.S. Embassy siege to the government of Iran, it should be proven that the militants have acted on behalf of the government and charged by some of the government's competent organs to do a certain operation.

In this regard, Jurist Ago stated in his separate theory in the Nicaragua case that the individuals or groups acting in the name or on behalf of the United States should have been charged particularly by the United States authority to do a certain act or do a particular mission on behalf of the United States.

While there is no disagreement regarding the first group or directions, the control criterion seems to be more of a problem since there are differences in the degree and amount of control in the procedure. The Court first spoke about the control criterion when mentioning the necessity of an accurate examination in the Nicaragua case. This means that a cyber-attack done by an individual or a group will be assigned to the government if that government has had a direct impact on the individual or group for committing the attack. The difference between a case where the attack has been done by an institution under a government's effective control, and a operational organ, is that the former needs no relation or dependence in terms of having an effective control, and more importantly, the relationship is proven based on the degree of control implemented by the government during each action; while in the case operational organs, the relationship is proven based on the degree of overall control that the government implements on the individual. In the Tadic case, the Special Court of Yugoslavia introduced an alternative criterion with a lower threshold. In this case, the court distinguished between the cases where the control criteria is necessary for unorganized individuals and groups, and the organized groups where an overall control is enough. A government uses overall control over a group not to supply equipment and give financial support, but also interferes in the overall program of their military activities by coordinating and helping them with the program. In these cases, there is no need for the government to give orders to the leader or members of the group to do certain activities against the international law. Thus an "overall control" includes cases where the government uses its public authority on a group and its activities. For example, a cyber-attack will be assigned to the government if it is done by a group of hackers whom the government has technically helped or given other kinds of assistance and has organized their activities; even if there is no proof of any interference in a specific attack. An overall control is therefore different from effective control, since the latter requires control over a specific action. It is also different from operational organs since there is no relationship between the government and the institution being discussed.

In the case of Genocide in Bosnia, the court criticizes the "overall control" criterion and again emphasizes the "effective control" criterion. Therefore, it stated that the genocide cannot be assigned to Serbians since its government has not applied its effective control on the operations during the time they have happened. Regarding the conclusions that the Court has reached, only the cyber operations done by institutions under a government's effective control are to be assigned to the government.

[52]. Prosecutor V Dusko Tadic 'a/k/a' DULE (Appeal) ICTY – 94-1- A(15 JULY 1999),para.141(Tadic Appeal).

It seems that there is no accurate and uniform standard that can be guaranteed, but instead the degree of control can be different depending on the context where the subject of control is discussed. Such a different method about control has been supported by the international procedure and doctrine. First of all, the International Law Commission's Responsibility of States Plan uses control with no additional word in article 8, while suggesting in the explanation that there should be a degree of flexibility.[53]

Moreover, in article 55 in Responsibility of States Plan, specific regimes are identified that have their own rules about the potential for assignment and responsibility.[54] As far as it was related to the international procedure, the effective control criterion was used for the Nicaragua case in terms of responsibility for humanitarian rights violation. The Court had to answer the question of whether violation of humanitarian rights through controlling can be assigned to the United States and creates international responsibility for them. For its own part, the Special Court of Yugoslavia used the overall control criterion for classifying war as international and not international. In search of an essential criterion in humanitarian rights, the court decided to refer to the assignment standards which can be found in rules about the responsibility of states. It introduced the overall control criterion only when it concluded that the humanitarian rights do not contain any specific rule in this regard. The reason why the special court of Yugoslavia disagreed with the rights about responsibility of states and introduced the overall control criterion was that in their view, the criterion was more reasonable in the condition of the case which was being examined.

The International Court of Justice used the effective control criterion for responsibility of the states in the case of genocide in Bosnia. The court also announced that the rules regarding the assignment will not change with the wrongful action discussed in the absence of a specific rule. This comment was stated because it was suggested that the criterion for the assignment potential should change in the case of responsibility for genocide.

Considering the overall control criterion in the case announced by the special court of Yugoslavia, the court accepted that this criterion can be suitable for using and that accepting a similar criterion for solving two different issues which are very different in terms of nature and essence (i.e. describing a contrast/ the responsibility of the states in genocide) has no place in appropriate logic. It is said that the International Court of Justice refused the "overall control" criterion for the rights of responsibility of states, since it develops the relationship that should exist between the behavior of a government's organs and its international responsibility.

The matter above shows the difference between two systems using the assignment potential criterion. On another hand, the basis of the responsibility of the state is that the governments are taken responsible for their wrongdoings. But this regime proposes a new and limited definition of the "state" and only assigns to it which are done by institutions closely related to the state. Meanwhile, it identifies different types of responsibility considering the different ways through which a government/state can interfere in wrongful action.[55] There are also different legal, criminal, national or international processes where the employees or subordinate institutions are also taken responsible.

The basis that exists beyond the regime of using force, on the other hand, is to present a pattern based on which force can be legally used in international relations. Anyhow, the regime of using force is rather government oriented. Even today there are nongovernmental actors who can use a high amount of force against other governments. These are present in governments and act from within a government. As the International Court of Justice stated, it is important to realize the reality of the relationship between the individual who takes an action and the government. Therefore, any kind or degree of control which is used over a nongovernmental actor by the government and leads to an attack against another government is enough for the target government to use force through self-defense against the enemy. This situation can be distinguished from a situation where a government uses no control over the nongovernmental actor because it is not able to apply its authority over its whole realm or the nongovernmental actors. In these cases, the target government can use force to directly defend itself against the nongovernmental actor.[56] This rule has been created in common international law. Based on the Caroline case (which is brought up as a reference of common law in self-defense) a government can use force

53. J Crawford, The International Law Commission's Articles on State Responsibility (Cup2001), p.112.

54. E.g. Article 3, The Hague's Fourth Convention, and Article 91, Geneva Conventions' Additional Protocol in August 12, 1949 regarding the first protocol (Supporting the victims in the international armed conflicts that opened for endorsement in June 8, 1977 and was called necessary in December 7, 1979. UNTS declares absolute responsibility to be humanitarian, where a state is responsible for all the actions of the individuals who create a part of the armed forces. See also article 59, the International Law Commission plan for responsibility of states)

55. E.g. see article 16 of International Law Commission's Plan for Responsibilities in 2001.

56 .N Tsagourias, Non- State Actors and Use of Force, in J d'Aspremont (ed). Participants in the International Legal System: Multiple Perspectives on Non- State Actors in International Law, (Routledge 2011) 326ff.

against nongovernmental actors through self-defense. Moreover, based on article 51 in the charter, starting the attack in a defense is determined based on the events and not the causes of the attack. The governments' new procedure regarding terrorism also confirms this method of self-defense. For example, following the attacks of Hezbollah which the Lebanon government could not prevent, Israel used this position to employ self-defense against Hezbollah in Lebanon in 2006. Not only did Lebanon deny any awareness about the attacks, but it also stated that it could not tolerate the attacks. In turn, Israel announced that its actions have not been against the Lebanese government and were done against Hezbollah. This subject of course reflects the Western view that sees Hezbollah has a terrorist group, but in Iran's specific viewpoint, Hezbollah is considered to be a national movement of liberation and therefore, Hezbollah's activities are not applicable to terrorist actions; thus Israel's use of legitimate law does not have a legal basis.

On the other hand, the International Court of Justice's declaration about self-defense being "only possible against a government's armed attack against another government"[57] is strange and has been criticized by other jurists in their own theories and comments.[58] According to Jurist Kooijman, if the armed attacks are conducted by unorganized groups from such a country against a neighboring country, they are still considered as armed attacks, even if they are not to be assigned to a land's government. It will not be logical to deny the rights of the target government just because there is no attacking country, and the charter has not considered this to be necessary either. The International Court of Justice had another chance to deal with the issue of nongovernmental actors, but it refused to express any certain opinions. In the case of Congo against Uganda, Uganda claimed that the country's actions against the riots that were being performed in the Democratic Republic of Congo are self-defenses due to the DRC's lack of ability to control its own territory.

Nevertheless, the Court announced that Uganda's actions were inappropriate and therefore felt that there was no need to comment on the legitimacy of the defense in reaction to the attacks of the unorganized forces.[59] It may be claimed that Uganda's reaction was appropriate and was considered as a legitimate self-defense, but there are disagreements in this regard.

The International Court of Justice's assessment that for the attack to be assigned to the government, the cause of the armed attack should be a government and that government should employ its "effective control" over the nongovernmental actor, may dominate the original purpose of maintaining international peace and safety, since the nongovernmental actors will be able to attack another government while remaining immune and being able to hide behind the shield of the hostile government. Conversely, the governments will also be able to perform attacks in the guise of nongovernmental actors.

3.2.3 State Toleration or Unwillingness

As the cases of terrorist attacks have shown, cyber-attacks may be performed against governments by nongovernmental actors in a governmental land where the governments tolerate them in their land or are too passive to stop their activities. According to international law, a government should not allow anyone to use its land for activities against the rights of other governments[60] and particularly, the government's land should not be used for military actions against another government.[61]

This rule results into creating a duty for a government based on which it should try its best in this regard; otherwise, if the government fails, it will have an international responsibility. Anyhow, if a harmful action leads to an armed attack, the issue will change the situation's legal state and the land will be considered to be in the domain of using force. The problem in this case is whether a government damaged by a cyber-attack is able to use force against a nongovernmental actor who has attacked from the land of another government and has been tolerated in another land. If the International Court of Justice's "effective control" criterion is to be used in this case, the target government will not be able to defend itself. Nevertheless, this will not be much of a consolation for the target government to know that it is able to either take the hostile government responsible for violating its obligations in trying to prevent those actions, or counteract against that government, but it will not have the right

[57]. Palestinian Wall, op. cit., para, 139.

[58]. Palestinian Wall : Separate Opinion of Judge Higgins, op. cit., para. 33; Declaration by Judge Buergenthal, op. cit., para. 6; Separate Opinion of Judge Kooijman, para.35.

[59]. Congo V Uganda, op. cit., para. 147.

[60]. Corfu Channel Case, op. cit., 22; Council of Europe Convention on Cybercrime (23 November 2001); GA RES 55/63 (22 January 2001).

[61]. The Alabama Claims (United State V Great Britain) 1872 Reprinted in JB Moore, History and Digest of International Arbitrations to which the United States has been a Party, Vol. 1 (6PO1898), 495 ff.

for self-defense.[62]

If we believe in having a duty of doing our best to maintain the important international virtues such as maintaining international peace and safety or doing some important obligations such as refusing to use force, it will not be logical not to allow the target government to defend itself against an armed attack which has happened due to another government's failure in trying to prevent those actions.

The assignment criteria, such as tolerating an action against the international law by a government or the government's passivity in preventing a wrongdoing has developed in the regime of force for concealing situations which have been discussed in the previous sections: cases that are not just assumptions, but are real and the international society suffers from them, e.g. cases of terrorist attacks that have happened in different parts of the world.[63]

For instance, when Al-Qaeda performed the attacks of September 11 and the Taliban regime refused to refund the Al-Qaeda leaders, The United States reacted through self-defense by use of force. The basis of this event had been provided in the statements of the Security Council beforehand, which asked the Taliban not to help international terrorists and take actions that would prevent the terrorists from using the U.S. land.[64]

The U.S. President justified the 2001 action based on self-defense, and declared that there is no difference between the people who have performed the attacks and those who have given them shelter.

In a letter to the Security Council, the United States of U. S. wrote the following about its actions in implementing the right of legitimate defense:

> The attacks of September 2001 and the resumption of threats from Al-Qaeda against the U.S. and its nationals, and the Taliban regime's decision to allow Al-Qaeda to use part of that country for its terrorist activities, shows this government's responsibility. And despite all the efforts done by the U.S. and the international society, the Taliban regime still refuses to change its policies.[65]

This position was supported in the Security Council's statements of 1368 and 1373 in 2001. The statements also confirmed the inherent right of individual or collective self-defense against the attacks.

In the case of Congo against Uganda, it seems that the International Court of Justice has examined the situation of tolerating nongovernmental actors and that if they cause an attack to another government, the situation can result into the right of self-defense; even though in that particular case the Court failed to make the conclusion that no action from part of the Democratic Republic of Congo equals the government's tolerance.

In summary, tolerating nongovernmental actors by a government leading to cyber-attacks against other governments, or a government's passivity in stopping the cyber-attacks which results in causing harm to other governments create the right of self-defense against the opposite. This criterion has been created by making the government responsible for its territory and nationals.

4. Conclusion

Nowadays, with the technological developments, especially in cyber area, the classical attacks are no longer the only options in battlefields, and cyber-attacks are increasingly evolving with the progression of technological abilities in different countries. The international law should also keep up with these trends, and should be able to answer the legal issues ahead of the international society by regulating specific laws in this area along with the technological advances. Until that day, the existing laws will be used in order to define new concepts. Article 2 in paragraph 4 of the charter regulating the rules regarding the use of force, and article 51 which regulates the right of self-defense, are examples of the rules which are used in this context. Therefore, cyber-attacks performed with the purpose of causing direct and physical harm or cause damage or death to the humans are classified under the use of force. In order for a target government to have the rights of self-defense against such attacks, the actions should reach the threshold of an armed attack. On the other hand, any kind of defensive action against such attacks should have the conditions of necessity, proportionality, and urgency. Moreover, another important issue in the area of using force and self-defense against such attacks is the way of assigning the responsibility to the governments committing the attacks. Due to the technological and technical

[62]. ME O'Connell, cyber security without cyber war's 4.1.

[63]. B Simma (ed), The of the United Nations, A Commentary, Vol. 1 (2nd edn, oup 2002) 802.

[64]. SC RES 1276 (15 October 1999), para. 1.

[65]. Letter from the permanent Representative of the United State of America to the United Nations addressed to the President of the Security Council (7 October 2001) S/2001/946 and Letter from the Charged, affairs of the Permanent Mission of the United Kingdom of Great Britain and Northern Ireland the United Nations addressed to the President of the Security Council (7 October 2001) S/2006/1947 (2001).

complexities in the cyberspace and the attacks performed in this area, assigning the responsibility will be a difficult task to do. Generally, the actions of the government's official organs, such as cyber army and operational organs, and private individuals such as hackers who are under a government's overall control, or the ones over whom the government makes no effort in controlling, can provide the basis of assigning responsibility to the governments.

References

Antolin-Jenkins, V. M. (2005). Defining the parameters of cyber war operations: looking for law in all the wrong places. *Naval L. Rev.*, *51*, 132.

Barkham, J. (2001). Information warfare and international law on the use of force. *NYUJ Int'l L. & Pol.*, *34*, 57.

Bowett, D. W. (1958). Self-defense in international law. Manchester University Press.

Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of Congo V Uganda) [2005] [ICJ].

Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA) (Merits) [1986].

Case Concerning Oil Platforms (Islamic Republic of Iran V USA) (Merits) [2003] [ICJ].

Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina V Serbia) [2007] ICJ.

Clark, D. D., & Landau, S. (2011). Untangling attribution. *Harv. Nat'l Sec. J.*, *2*, 323.

Condron, S. M. (2006). Getting it right: Protecting American critical infrastructure in cyberspace. *Harv. JL & Tech.*, *20*, 403.

Corfu Channel (United Kingdom V. Albania) (Merits) [1949] [ICJ].

Crawford, J. (2002). *The International Law Commission's articles on state responsibility: introduction, text and commentaries*. Cambridge University Press.

Creekman, D. M. (2001). Helpless America--An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China, A. *Am. U. Int'l L. Rev.*, *17*, 641.

Dinstein, Y. (2011). *War, aggression and self-defense*. Cambridge University Press. https://doi.org/10.1017/CBO9780511920622

Draft Articles on the Responsibility of States for Internationally Wrongful Acts (Draft Articles) by the International Law Commission (ILC) in August 2001.

Gill, T. D. (2006). The temporal dimension of self- *defense*: anticipation, pre-emption, prevention and immediacy. *Journal of Conflict and Security Law*, *11*(3), 361-369. https://doi.org/10.1093/jcsl/krl018

International Committee of Red Cross Customary International Humanitarian Law Study, Vol. 1, Cambridge University Press. 2005.

International Military Tribunal (Nuremberg) Judgment of 1 October 1946.

O'Connell, M. E. (2006, March). Rules of Evidence for the Use of Force in International Law's New Era. In *Proceedings of the Annual Meeting (American Society of International Law)* (Vol. 100, pp. 44-47). American Society of International Law.

Reisman, W. M., & Armstrong, A. (2006). The past and future of the claim of preemptive self-defense. *American Journal of International Law*, 525-550.

SC RES 1276 (15 October 1999).

SC Res 1310 (27 July 2000).

SC Res 1337 (30 January 2001).

SC Res 1553 (29 July 2004).

SC Res 1559 (2 September 2004).

Schmitt, M. N. (1999). Computer network attack and the use of force in international law: thoughts on a normative framework. *Columbia Journal of transnational law*, *37*, 1998-99. https://doi.org/10.21236/ADA471993

Schmitt, M. N. (2010). Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. In *Proceedings of a Workshop on Deterring Cyber-attacks: Informing Strategies and Developing Options for US Policy* (Vol. 151, pp. 163-64).

Simma, B. (Ed.). (2002). *The Charter of the United Nations: a commentary* (Vol. 2). Oxford: Oxford University Press.

Tallinn Manual on the International Law Applicable to Cyber Warfare," Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defense Center of Excellence, General Editor: Michael N. Schmitt, Cambridge University Press, New York, 2011.

The Alabama Claims (United State V Great Britain) 1872.

Tsagourias, N. (2012). Cyber-attacks, self-defense and the problem of attribution. *Journal of conflict and security law*, krs019. https://doi.org/10.1093/jcsl/krs019

United States Diplomatic and Consular Staff in Tehran (United States of America V. Iran) [1980] [ICJ].

Wilmshurst, E. (2006). The Chatham House principles of international law on the use of force in self-defense. *International and Comparative Law Quarterly*, *55*(04), 963-972. https://doi.org/10.1093/iclq/lei137