مركز البيدر للدراسات والتخطيط
Al-Baidar Center For Studies And Planning

Cyber Attacks And State Responsibility for Them

Zahraa Imad Muhammed Kalanter

Al-Baydar Center Publications for Studies and Planning

About Center

Baidar Center for Studies and Planning is a non-governmental and non-profit organization established in 2015 and registered with the NGO Directorate in the General Secretariat of the Council of Ministers in Baghdad.

The Center seeks to contribute to developing the state and its institutions, by proposing ideas and practical solutions to the main problems and challenges facing the state, including improving public sector management, policies and strategic planning, using reliable data and best practices. The Center engages the relevant authorities in the state with regular meetings to support this objective and utilises the support of international organizations dedicated to assisting Iraq's developmemnt. The Center also seeks to support economic reforms, sustainable development and provide technical assistance to the public and private sectors. The Center also seeks to support development of the private sector to provide job opportunities for citizens through training and upskilling, in a way that reduces dependence on government institutions and contributes to supporting and diversfying the country's economy.

The Center aims to utilise the vast amount of potential in Iraq's human resources by organizing programs to prepare and develop promising young people, including leaders capable of proposing, adopting and implementing visions and future plans that advance society and preserve its value system based on the commitment to a high moral standard and rejection of all types of corruption.

Cyber Attacks And State Responsibility for Them

Zahraa Imad Muhammed Kalanter

Introduction

The nature of life is continuous change, and our era is currently characterized by its ever-increasing speed, through the development of human societies that often go through historical turns determined by revolutions in science and technology, the development of available means of production and their repercussions on society, and as an extension of these sharp turns in human history, now we are witnessing a new revolution in the communications sector, especially in the field of information technology.

The increasing reliance on the Internet in most aspects of life, such as economy, culture and society, has increased the risks as well. This development has allowed new ways of international interaction that were not noticed or expected when establishing the prevailing legal systems. After international dealings during armed conflicts take place on the ground or Air or sea, thanks to these technologies, is done electronically within an information system completely different from traditional armed conflicts, and cyberspace has become a real competitor to the traditional international scale, and the threat of cyber attacks has begun to loom more than ever and with the increasing global reliance on digital technology, increased also the exposure to attacks on critical infrastructure through cyberspace.

Cyber attacks have become one of the effective ways and methods without significant costs. After the traditional system relied on human military power to confront the rest of the countries or control them by land, air, or sea, which costed the countries a lot of human and material losses and required time and effort, the international information system (cyber) depends mainly on electronic means for all the affairs of individuals and societies, and countries can influence others and paralyze their banking, security or military system with the push of a button from afar without incurring the trouble and without causing human losses in their ranks. However, the destruction they achieve in the attacked country may outweigh the

effects of the traditional armed conflict, whether in the loss of human lives or the destruction of infrastructure.

Although the exact parameters of cyber-attacks are still undetermined, the massive attacks against information infrastructure and Internet services in the last decade give some picture of the potential shape and scope of conflict in cyberspace, and cyber-attacks have become one of the most important existing challenges, and a new concept of the current hidden warfare, and visible in the near future as an alternative to conventional war.

What are Cyber Attacks?

The rapid development in information and communication technology has led to the dependence of societies in various political, security, social and economic dimensions on computer networks and the Internet.

This development was not without risks, as the low cost, communication network software gaps, and the difficulty of identity detection, allow states, and even non-governmental entities or individuals, to attack the networks of other countries and damage their information and vital infrastructures, such as disrupting electricity networks and Disrupting the communications system and destroying aircraft, and other infrastructure that depends in its operation and work on computer networks and the Internet. With the increasing reliance on the Internet, especially in areas related to national security such as military and security networks, there has been increased talk about the importance of confronting these threats. In this context, the concept of cyber-attacks emerged, which are electronic actions carried out by countries or their affiliates against computer systems and networks belonging to other countries for security or military purposes[1]. And cyber attacks have become one of the main challenges and threats that countries must face in the current era.

First: the Definition of Cyber-Attacks

The definitions of existing cyber attacks and related concepts are very broad, but there are two main different directions[2] in defining this type of attack, namely the narrow trend and the broad trend. The narrow trend focuses on the issue of the attack, and this is what the United States of America and its allies have

1.Oona A. Hathaway, Rebecca Crootof , Philip Levitz, Haley Nix, Aileen Nowlan , William Perdue & Julia Spiegel, «The law of Cyber-Attack», California law review, 2012, p.824.
2.«United States Cyber Command».

adopted. Examples of definitions in this direction are what was mentioned in the Dictionary of Military Uses published by the Joint Chiefs of Staff in 2011 after the establishment of the "American Cyber Command"[3], where a cyber attack was defined as: "A hostile activity using a computer, networks, or related systems, aimed at to disable or destroy the adversary's critical cyber systems, property, or functions. The intended results of a cyber attack are not necessarily limited to the targeted computer systems or the data themselves, and the activation or effect of a cyber attack may separate in time or space from the cyber activity"[4].

In contrast to the narrow line officially adopted by the United States, the Shanghai Cooperation Organization[5] has taken a more expansive approach to cyberattacks. Where this organization expressed its concern about the threats posed by the possibility of using modern information and communication means and technologies for purposes incompatible with ensuring international security and stability at the military and civil levels[6]. Members of this organization – that is, supporters of the broad trend – view the dissemination of harmful information to the social, political, social and economic systems, as well as the spiritual, moral and cultural spheres of other countries as also major threats to cybersecurity[7].

The conflict in the content of these two trends – the concept of cyber attacks – shows the urgent need for a clear and internationally agreed definition of these attacks.

The cyber attack is a behavior that takes place in a digital world based on the use of digital data and electronic means of communication, and then developed to include a broader concept based on achieving concrete and direct military or security objectives, as a result of penetrating sensitive websites, which usually

3.James E. Cartwright, Memorandum for Chiefs of the Military Serve. Commanders of the Combatant Commands, Dirs. Of the Joint Staff Directories on Joint Terminology for Cyberspace Operations 5 (No. 2011).

4.The Shanghai Cooperation Organization (SCO) was established in Shanghai on June 15, 2001 and became an official organization in accordance with the principles of international law in 2002. It consists of China, Russia and most of the former Soviet Union republics in Central Asia, as well as observers, including Iran, India, Pakistan March 2013. Available at http://lcis.Uobaghdad.edu.iqLuploads/workshop/

5.Oona Hathaway, op, cit p.825.

6.Shanghai Cooperation Agreement, Annex I, p. 203.

7.Ahmed Obais Ne'ma Al-Fatlawi, "Cyber attacks their concept and the international responsibility arising from them in the light of contemporary international organization", Al-Mohaqiq Al-Hilli Journal for Legal and Political Sciences, Babylon University, the eighth year, No. 4, 2016, p. 616.

perform functions classified as priority, as the systems that protect the nuclear or electrical power plants, airports and other means of transportation[8]). Therefore, we see that the definition provided by "Schmidt", a specialist in international humanitarian law and a prominent member of the NATO Cooperative Cyber Defense Center (NATO) in the Tallinn Guide is the closest to the concept of cyber attacks, as he defined them by saying: "A cyber attack is any electronic action, whether defencive or offensive, it is reasonably expected to cause injury or death to a person, or material damage or destruction to the attacked object"[9].

This definition is consistent with what was stated in the Council of Europe Convention on Cybercrime of 2001, where Article 5 (5) of it states: "Each State Party shall adopt such legislative and other measures as may be necessary to criminalize the following act in its national law, if it is committed intentionally. Unrightfully, seriously obstructing the functioning of a computer system by inserting, sending, destroying, erasing, changing, altering or destroying computer data"[10].

Second: **The Nature of Cyber Attacks**

When referring to the definition of cyber-attacks, several questions arise regarding the nature of these attacks. Is it correct to consider it an attack in the idiomatic sense? Can a cyber attack be considered a combative method, or is it considered a combative method?

To answer these questions, it is necessary to refer to the provisions of the international instruments related to the regulation of traditional armed conflicts. So (attacks) as mentioned in international humanitarian law are acts of violence against an opponent, whether they are carried out as an attack or defense, regardless of the region in which those acts are carried out, and this is what was stipulated in the First Additional Protocol to the Geneva Conventions of 1977 in the first paragraph of Article (49) as: "Attacks mean offensive and defensive acts of violence

8.Michael N. Schmitt. William H.Boothby. Wolff Heintschel Von Heinegg. Thomas C.Wingfield. Eric Talbot Jensen. See Whatts. Louise Arimatsu. Genevieve Bernatchez. Penny Cumming. Robin Geiss. Terry D.Gill. Derek Jinks. Jann Kleffner. Nils Melzer & Kenneth Whatkin, «Tallinn Manual on the International Law Applicable to Cyber warfare», Cambridge University Press, First Publishes, 2013, p. 92.

9.Council of Europe, "Council of Europe Convention on Cybercrime, European Treaty Series No. 185, Budapest, 2001, Article No. (5).

10.International Committee of the Red Cross, "Annexes" to the Additional Protocols to the Geneva Convention of 12 August 1949, Geneva, Switzerland, 4th edition, 1997, p. 40.

against an opponent"[11].

As for the cyber activities in question, according to this definition, they are not considered as an attack. Hacking and penetration of electronic data, even if they are directed at the opponent for attack or defense, do not involve acts of violence, and accordingly, if we take the text of this paragraph in isolation from the rest of the provisions of the protocol, cyber activities with destructive effects cannot be described as offensive. But this is not correct, as it is not possible to read the text of the first paragraph of Article (49) in isolation from the rest of the provisions of the protocol, which stipulates in other articles the basic rules governing attacks that can apply to some extent on cyber attacks, such as the rule contained in Article (48) which requires the conflicting parties to always distinguish between civilians and combatants and between civilian objects and military objects, ie: in other words, it prohibits indiscriminate attacks[12]. This is confirmed by the seventh rule of international humanitarian law, which states that "the parties to the conflict shall distinguish at all times between civilian objects and military objectives"[13], and also what Article (51) in the second paragraph contains regarding the prohibition of attacks against the civilian population that are primarily aimed at To spread terror among them[14]. As well as the prohibition of attacks on installations containing dangerous forces that may cause damage to the natural environment and thus endanger the health and safety of the population as contained in Articles (52 and 56) of the same protocol[15].

From the foregoing it becomes clear that armed violence acts are of two types[16]: they are either: direct, and by their nature lead to material harm to military and civilian targets, or indirect, that is: they cause harm after the attack, whatever the means or method.

According to the foregoing, focusing on the effects and severity of cyber

11.The previous source, pg.

12.John-Marie Henkerts and Wisdoswald-Beck, Customary International Humanitarian Law, International Committee of the Red Cross, Volume I (Rules), p. 23.

13.International Committee of the Red Cross, «Annexes», the Additional Protocols to the Geneva Convention of 12 August 1949, previous source, p. 40.

14.The previous source, pp. 41 and 42.

15. Ahmed Obais Nima Al-Fatlawi, previous source, pg. 617.

16.Laurent Gesell, What are the Law of War Restrictions on Cyber Attacks, International Committee of the Red Cross, 06/28/2013. Available on the official website: (last visit on 5/8/2016) https://www.ICrc.org.Cyber-warefare.

activity will show whether the description of the attack is fulfilled, for example when computers or networks in a country are subjected to a cyber attack, this may lead to depriving civilians of basic needs such as drinking water, medical care and electricity.

Cyber activities can interfere with the disruption of life-saving services such as hospitals or critical infrastructure such as dams, nuclear reactors and aircraft control systems, and as a result hundreds of thousands of people may be affected[17]. These activities, according to their severity and effects, whether direct or indirect, are considered a cyber-attack, that is, the description (attack) applies to them.

Adapting Cyber Attacks

One of the most important aspects of combating this growing threat is the adaptation of these attacks, and the identification of the responsibility of states, whether they commit them directly through their security and military services, or those that implement them by supporting other groups that are not officially affiliated with them. Accordingly, cyber attacks must be adapted under both the law of war (Jus ad Bellum), which exists between the folds of public international law, and the law in war (Jus in Bello) or international humanitarian law, because international law distinguishes between the causes of armed conflict and armed conflict themselves. This distinction constitutes a crucial element in ensuring respect for both laws[18]. The purpose of international humanitarian law or the law of war is to protect the victims of armed conflicts regardless of their affiliation to the parties to the conflict or the extent of the conflict's legitimacy. It is limited to regulating aspects of the conflict of humanitarian importance and Its provisions apply to the warring parties regardless of the fairness of the cause defended by this or that party, unlike the law of war, which examines the legality of armed conflict and seeks to restrict the use of force between states, and this is the reason for the importance of distinction and independence of the law of war from Law in War[19].

On the other hand, the disagreement of the jurists regarding the concept of

17.François Bunyon, Just War, War of Aggression and International Humanitarian Law, International Review of the Red Cross, Selections from 2002 Edition, pp. 36-41.

18.International Committee of the Red Cross, International Humanitarian Law (Answers to Your Questions), December 2014, pp. 8-9.

19.Parviz Hosseini and Hossein Zarif Manesh, The Structure of Cyber Defense in Countries A Comparative Study, Journal of Gohshahi-Hafti-Amniti, Imam Hossein University (Peace be upon him), Tehran / Iran, second year, No. 5, 2013. p. 52.

these attacks leads to their differing opinions on the laws applicable to them. There are those who believe that international laws and instruments regulating armed conflicts were developed before the impact of electronic systems on the means and methods of combat, and the authors of these systems did not take technological developments into account, and therefore cyber attacks are not subject to these instruments and rules. On the contrary to this view, another group argued that these rules are flexible and can be applied to cyber attacks as well[20].

First: **Cyber Attacks Under the Law of War** (**Jus ad Bellum**)

The Law of war refers to the circumstances in which states can resort to armed conflict or the use of armed force in general: in other words, it examines the legality of resorting to the use of armed force[21] . In order to build a peaceful world, the UN Charter affirms the settlement of disputes by peaceful means, the prohibition of acts of aggression and the prohibition of the threat of force against any state[22].

Cyber attacks pose a threat to the main principles of international law, such as respect for the sovereignty of states, because of the penetration of security and military information classified as confidential, and undermine a basic duty, which is to refrain from using or threatening to use force due to its severe damage to the functioning of the government and services in the country that is exposed to such attacks[23]. Based on the foregoing, we will discuss the adaptation of cyber attacks according to the law of war in light of its basic principles in the following two sections:

Section I: **The Principle of Sovereignty**

The idea of sovereignty and its recognition of states is one of the principles agreed upon in the Charter of the United Nations and international agreements that are relevant in this regard. The first paragraph of Article 2 of the Charter of the United Nations referred to the principle of sovereign equality of all its members by text: "The Commission is based on the principle of sovereign equality of all its

20.International Committee of the Red Cross, International Humanitarian Law (Answers to Your Questions), December 2014. p. 8.
21.Charter of the United Nations, Chapter One, Articles 1-2, on the official website: www.un.org>charter-united-nations.
22.Muhammad Ali Rait Cunnindh Falah, Cyber War and the threat to the national security of the Islamic Republic, PhD thesis, Islamic Azad University, College of Arts and Humanities, Download / Iran, Iran, 2012, p. 72-76.
23 Charter of the United Nations, Chapter One, Articles (2) P1.

members"[24]. In light of the technological change and the emergence of cyberspace, the traditional concept of sovereignty has changed through the emergence of new concepts, including what is known as digital sovereignty, which is defined as "the extension of the state's control and jurisdiction over the digital space represented by the Internet, which crosses the borders of the state and creates a group of virtual people within electronic networks beyond any national affiliation"[25]. Here the real challenge emerged, as the state cannot impose its control over its citizens in cyberspace through nationality, for example, and cyberspace is not limited to encompassing traditional geographical concepts, but extends to include the phenomenon of absenteeism of national identity[26].

Users of computer networks and the Internet, that is: individuals who make up the cyberspace belong to multiple political communities, and in the event that a crime is committed within this space and the state tracks the source of the crime, the concept of national sovereignty may be violated for this, as the source of the crime may belong or fall within the scope of sovereignty of another country. Based on the foregoing, it can be said that the traditional state sovereignty and its components are beginning to diminish with the presence of electronic means of communication that make the territorial borders of states and national affiliations diminish little by little, which raises the question about the scope of state sovereignty in cyberspace[27].

The erosion of geographical borders in the cyberspace, made some of them see that this takes the cyberspace out of the control and sovereignty of the state, and leads to the absence of the rule of law in it, but this is not true at all for several reasons, including:

1- The use of cyberspace requires physical devices and equipment without which users cannot access it, and since this physical structure is located within the

24. Sarab Thamer Ahmed, Attacks on Computer Networks in International Humanitarian Law, a dissertation from the requirements for obtaining a PhD in Public Law, Al-Nahrain University, College of Law, 2015, p. 101.
25. Nabil Ali and Fadia Hijazi look at the digital divide, an Arab vision of a knowledge society, Knowledge World Series, No. 318, (Kuwait, The National Council for Culture, Arts and Letters, 2005), p. 12.
26.Mustafa Essam Naous, State Sovereignty in Cyberspace, Journal of Sharia and Law, United Arab Emirates University, College of Law, Twenty-sixth Year, Issue 51, July 2012., pp. 136-139.
27.See Joshua E. Kastenberg, Non Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law, 64 Air Force Law Review.

territory of the state, it is natural that it falls within the jurisdiction of that state, and thus the state imposes its control and sovereignty over it.

On the other hand, the cyberspace itself requires regulation and oversight with regard to the names of users, their addresses, and the launch range of the electronic communication signal[28], and this regulation is subject to the control and supervision of the state.

2- The financial relationships that arise through cyberspace need laws regulating them, otherwise they become weak and unreliable[29].

3- The contents and information sent through cyberspace have importance in the real world, that is, the state has a declared interest in controlling the information that flows through this space and in particular in protecting its citizens from defamatory statements or protecting public order and morals from pornography, this information must To be subject to the laws of the country in which it is located to protect its interests[30].

4- The ability to cause damage, create chaos, or spread violent or hate speeches (speech of hate) through cyberspace, is very similar to real world risks and countries have always perceived cyberspace as a matter of national security, which requires finding the means possible to impose control and reduce its risks[31].

The aforementioned reasons refute the saying that cyberspace is far from the sovereignty of states, and therefore states have begun to address the problems of sovereignty, in order to avoid future risks as a result of the use of cyberspace, whether at the national or international levels. The majority of them developed their national legislation to accommodate the crimes that occur within their territory and coordinated with other countries by concluding agreements dealing with the regulation of cyber crimes and solving the problem of sovereignty by agreeing on mechanisms to track sources of crime and the laws to be followed in

28.Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, (Oxford Univ. Press, 2006).

29.Jack L. Goldsmith & Tim Wu, Who controls the internet? Illusions of a borderless world, op.cit, P. 147-61.

30.Patrick W. Franzese, Sovereignty in Cyberspace: can it exist? University of Pennsylvania Law 20/6/2014 available at: http://www.law.upenn.edu/live/files/3473-Franzese-p-sovereignty-in-cyberspace-can-it-exist. (last visit on 8/29/2016).

31.Recommendation of the Council of Europe No. R(95)13 of 11 September 1995.

the event of their occurrence, such as the recommendation issued by the Council of Europe on problems Procedural information related to information technology[32], the Budapest Convention of 2001[33], the Strasbourg Protocol of 2003[34]), and the Arab Convention against Information Technology Crimes of 2010[35].

In general, the principle of territorial sovereignty applies to cyberspace and includes electronic infrastructure, whether it is on the territory of the state, its internal waters, its territorial sea, or even its archipelagic waters. The state has the right to exercise control over cyber infrastructure activities, such as computer systems, communication and information networks and energy sectors, transport and .... In those areas, taking into account that the exercise of that sovereignty can be regulated in accordance with the customary or codified rules of international law[36]. NATO experts have gone further, asserting that states have a duty to prevent cyber infrastructure located in their territory or under their full control (Overall Control) from being used in activities that infringe on the sovereign rights of other states[37]. And through the foregoing, it can be said that the state's sovereignty over the cyber infrastructure is not limited to that located or built on the state's territory, but extends to all cyber infrastructure that is completely under its control, even if it is in the territory of another state[38].

In light of the above, cyber-attacks directed by a particular state against the cyber infrastructure of another state, could represent a breach of the sovereignty of the territorial state, especially if these attacks cause devastating effects[39].

32.Council of Europe, Council of Europe Convention on Cybercrime, European Treaty Series No. 185, Budapest 2001.
33.Additional Protocol to the Information Crime Convention on the Criminalization of Acts of a Racial and Xenophobic Nature Committed Through Computer Systems, January 28, 2003, at http://Conventions.Coe.int/treaty/fr/Treaties/Html/189.htm.
34.) www.lawjo.net>showthread>26439.
35.Wolff Heintscble Von Heinegg, Territorial Sovereignty and Neutrality in cyberspace, U. S. Naval war college, 2013 volume 89, p. 128.
36.Tallinn Manual on the International law applicable to cyber warfare, charter.1, section. 1 , Rule. 5.
37.Tallinn manual on the international law applicable to cyber warfare, op. cit., p.27.
38.Mirage Thamer Ahmed, a previous source, p. 118.
39.United Nations Charter, Article 2 (Fourth).

Subsection Two: Prohibition of the Use or Threat of Force

Article 2 of the Charter of the United Nations states in its fourth paragraph: "All members of the Organization shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nation[40]. This prohibition is complemented by the non-interference rule of customary international law that prohibits states from interfering in the internal affairs of other states[41].

The International Court of Justice (ICJ) has confirmed in the Military and Paramilitary Activities case (Nicaragua v. the United States) that whenever the intervention takes the form of the use or threat of the use of force, the rule of non-interference contained in customary international law is consistent with Article 2 / IV of the Charter of the United Nations[42].

The scope of the UN Charter›s prohibition against the use or threat of using the force has been the subject of intense international debate. International legal scholars have gone to two different directions in determining the scope of the prohibition contained in Article 2/Fourth: The first group believes that the prohibition contained in the Charter is a broad prohibition and does not include only the use of military force, but includes all types of political and economic coercion, and this is what most support developing countries[43].

As for the other party, it relies on the narrow concept in the interpretation of this paragraph, and the prohibition is limited to armed force only, and this is what the great powers favor, especially those that support the concept of the responsibility to protect[44].

There are two consequences for this difference: The first is when a narrow opinion is taken, i.e. the prohibition is considered to include armed force only,

40.General Assembly. Res.37/10, U.N. Doc.A/RES/37/10 (Nov., 15, 1982) – also General Assembly Rec. 25/2625, U.N. Doc. A/RES/25/2625 (Oct. 24, 1970).
41.ICJ, Military and paramilitary activities in and against Nicaragua (Nicar .v. U.S.), 1986, ICJ. 14, (June 27), para. 209.
42.Daniel B. Silver, Computer Network Attack as a Use of Force Under article 2(4) of the United Nations Charter, in computer network attack and international law 73, 80-82 (Michael N. Schmitt & Brain T. O›Donnell eds. 2002).
43.Ibid.
44.Mirage Thamer Ahmed, a previous source, p. 111.

which leads to the inability of the state against which unarmed pressures, whether political or economic, regardless of their degree, to resort to the use of force under the pretext of self-defense.

As for the second picture, it expands the concept of force and gives the target state the right to respond to these interventions by all means, including the use of force in self-defense, whether individually or collectively[45].

As for the practices of the international community, it confirms its adoption of the narrow concept of force. It was stated in the judgment of the International Court of Justice in the aforementioned Nicaragua case: stated in the judgment of the International Court of Justice in the aforementioned Nicaragua case: "Mere economic or political pressure cannot constitute a use of force within the meaning of the Charter of the United Nations in Article (2/4)"[46]. The prohibition on the use of force contained in Article (2/4) is not absolute, but is subject to two exceptions: The first exception is in the matter of international peace and security contained in Article 39 of the Charter of the United Nations, which gives the authority to the Security Council to determine the existence of any threat or breach of peace or an act of aggression, and then he may decide the measures to be taken to maintain or restore international peace and security[47]. The Charter provides for the authority of the Security Council to take measures that do not involve the use of armed forc[48], or to act through land, sea and air forces[49].

Collective security measures under Article 39 may be politically difficult because they require authorization by the Security Council, whose movements are often slow due to the nature of interests among the permanent members[50].

As for the second exception to Article (2/4) it is regarding the right of legitimate defense mentioned in Article (51) of the Charter of the United Nations, where this Article states: "Nothing in this Charter weakens or diminishes the natural right of individual or group states to defend themselves if an armed force attacks a Member of the United Nations, until the Security Council takes the necessary measures to

45.ICJ , Military and paramilitary activities in and against Nicaragua (Nicar .v. U.S.), 1986, ICJ. 14, (June. 27), paras 188-190.
46.Charter of the United Nations, Article 39.
47. Previous source, Article 41.
48.Previous source, Article 42.
49.Oona Hathaway, op.cit., p. 814. (4)
50.Charter of the United Nations, Article (51).

maintain international peace and security."[51].

This article requires states to use their right to legitimate defense if they have been subjected to an armed attack. Hence, other forms of use of force that do not constitute an armed attack do not give the right to legitimate defence. Under these exceptions, the permissibility of the use of armed force depends on the occurrence of aggression, as the definition of aggression came in a resolution issued by the General Assembly of the United Nations as: "The use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with Charter of the United Nations»[52]. From the foregoing, the following question may come to mind: Do cyber attacks constitute an armed attack or another form of force? Does the exposure of a country to a cyber attack give it the right to legitimate defense?.

To answer these questions, it is necessary to address the main theories that emerged to determine when a cyber attack can be considered an armed attack, and then arranges the right to legitimate defense.

These theories are based on the following approaches:

1- The Instrument-Based Approach

The authors of this approach adopted the standard of the means used in the attack, and according to this theory, the cyber attack alone, will not create the concept of an armed attack that requires the right of legitimate defense contained in Article (51) of the United Nations Charter because it "lacks the physical characteristics associated with military coercion." In other words, because it generally does not contain kinetic energy (Kintinc) as is known in conventional weapons[53]. What supports this theory is what the United Nations has said regarding total or partial cutting off of the telegraph, radio and other means of communication are measures that do not require the use of force[54]. And the definition of aggression contained in a resolution of the United Nations General Assembly included in the third paragraph of it, a number of acts that would constitute "aggression, under Article

51. General Assembly, Res. 3314, U.N. Doc. A/RES/3314, (Dec. 14, 1974).
52.Michael N. Schmitt, Computer network attack and the use of force in International Law: Thoughts on normative framework, International Review of the Red Cross, No.846, 30/6/2002.
53.Charter of the United Nations, Article 41.
54.UN.General Assembly.Res. 3314, Dec,14,1974.

39 of the Charter"[55]), all of these actions, even if they are just examples, include the use of conventional weapons or military force. Nevertheless, the Security Council has the right to consider an act as aggression, even if the form of such aggression is not mentioned in the third paragraph of this resolution[56].

NATO has also indicated its support for this theory by stipulating in its 2014 Common Cyber Defense Approach: "A cyber attack will obligate Member States to "consult" with each other under Article 4 of the North Atlantic Treaty. …however, a cyber attack does not create an armed attack that obliges Member States to assist each other under Article (5) of this Treaty"[57]. This is a striking development, especially after the cyber attack on the Republic of Estonia in 2007, when NATO met in response to that attack in accordance with Article (5) of the NATO Charter, that is, the article that allows the use of armed force against any attack on a state party to it.

Although this theory is easy to apply due to the ease of defining weapons and military power, it overlooks cyber attacks that have the ability to cause great damage without the use of conventional military weapons ([58]).Although this theory is easy to apply due to the ease of defining weapons and military power, it overlooks cyber attacks that have the ability to cause great damage without the use of conventional military weapons[58].

2– Target–Based Approach

According to this theory, it is sufficient for a cyber attack to target a very important electronic system, in order to be classifed as an armed attack, and the owners of this theory focus on the nature of the target being targeted. The cyber attack needs to penetrate a major system, for example, the critical national infrastructures of the state such as banking systems, to justify the traditional military responses in confronting it, which can ignite a conventional war (Conventional

55. Badr Muhammad Hilal Abu Huaymel, The Crime of Aggression in International Law, A Study of Completing Success Requirements in the International Law Course, Al al-Bayt University, College of Graduate Studies, Jordan, 2012, p. 12.
56.NATO Agrees Common Approach to Cyber Defense, Fe. 25, 2014, available at: http://www.euractiv.com/en/infosociety/nato-agrees-common-approach-cyber-defence.article. 171377.
57.Oona Hathaway, op. cit., p. 846.
58.Matthew J. Sklerov, solving the Dilemma of state Responses to cyber attacks: A Justification for the use of Active Defenses against states who Neglect their Duty to prevent, 201 MIL. L. REV., fall 2009, at 1, 74-75.

War)[59], this theory has been criticized for ignoring the concept of critical multi-purpose infrastructure of the state in the current era, as well as the gravity of the cyber attack and its effects[60].

3-Effects-Based Approach

This approach is a middle approach between the means-based approach and the objectives-based approach. As the owners of this theory classify the cyber attack as an armed attack on the basis of the danger of its effect[61]. Some jurists who support this theory have identified the factors that can be measured against to classify a cyber attack as an armed attack, and among these factors are immediate, direct, and measurable risk factors[62], The owners of this theory also believe that every suspicious activity can be punished according to its effects on other countries[63].

Daniel B. Silver, former general counsel of the Central Intelligence Agency and the US National Security Agency, has stated that: "A cyber attack is justified in legitimate defense if its expected result is physical injury or material damage similar to the results associated with armed coercion"[64]. According to this theory, a cyber attack, for example, against the air navigation control system, and causing aircraft accidents, will be considered an armed attack because it is expected that such an attack will cause great losses, whether in lives or money. Marco Roscini endorsed this approach by saying, «...Cyber attacks may be considered a clear breach of the provisions of Paragraph 4 of Article 2 of the Charter of the United Nations, provided that they cause widespread disruption or destruction of infrastructure essential to the life of the human being, and if this is achieved, the offended state has the right to resort to the use of force according to Article 51 of the same charter,

59.Gray Sharp, in Stephanie G. Handler, The new cyber face of the Battle, Developing a Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law, vol. 48, 2012, p. 12.

60.Daniel. B. Silver,., Computer Network Attack as a Use of Force Under article 2(4) of the United Nations Charter, in computer network attack and international law 73, 2002, p.13.

61.Michael N. Schmitt, Computer Network Attack and the use of Force in International Law, op. cit., p. 914.

62.Sean P. Kanuck, Recent Development: Information warfare: New Challenges for public International Law, 37 Harvard International Law Journal, l. 1996, 272, 290.

63.Daniel B. Silver, op. cit., p. 89.

64.Marco Roscini, «World Wide Warfare- Jus ad Bellum and the Use of Cyber Force», Max Planck yearbook of United Nations law, vol. 14, 2010, p 85-130.

which provides for the right to self-defense"[65]. From the above, it can be said that this trend, although it is the most important and accepted trend of the previous theories, but it applies only to a small group of harmful cyber attacks, that is: those that have effects similar to the effects of the attack using conventional weapons or weapons of mass destruction[66].

As for the group of experts in the Tallinn Handbook, they went by saying that: "Any cyber attack using or threatening to use force against the territorial integrity or political independence of any country or in any way inconsistent with the purposes of the United Nations, is an unlawful act"[67]. They relied on the advisory opinion issued by the International Court of Justice on the legality of the use or threat of the use of nuclear weapons[68], which stated in one of its paragraphs that the prohibition of the use or threat of force contained in Article (2/4) of the Charter of the United Nations and the right of the legitimate defense contained in Article (51) of the same charter, applies to "any use of force regardless of the nature of the weapons used"[69].

Based on the foregoing, it can be said that cyber attacks, whenever their effects are similar to the effects of a traditional armed attack in terms of physical injuries and material damage, are adapted as a use of known armed force, and therefore the affected state resorts to using its right to self-defense[70] .

On the other hand, Article (2/4) did not prohibit the use of armed force only, but also prohibited the threat to use it against other countries. The threat to use force was defined as: «An explicit or implicit threat, verbally or in deed, of the unlawful use of armed forces against a state or several states, the realization of which is dependent on the will of the state that made the threat»[71].

Based on the provisions of the International Court of Justice in its advisory opinion on the legality of the use or threat of use of nuclear weapons in paragraph

65.Oona Hathaway, op. cit., p. 848.
66.Tallinn Manual on the international law applicable to cyber warfare, op.cit, Chapter II, section 1, Rule 10.
67.Ibid, p. 42.
68.ICJ nuclear weapons advisory opinion, legality of threats or use of nuclear weapons. Advisory opinion, 1996, I.C.J. 226 (8 July), para 39.
69.Tallinn manual on the international law applicable to cyber warfare, op. cit., p. 54.
70. Marco Roscini, «Threats of Armed Force on contemporary International Law». Netherlands International Law Review, No. 54, 2007, p. 235.
71.ICJ Nuclear weapons advisory opinion, op. cit., para 47.

47 that (the concepts of "threat" of force and "use" of force in accordance with Article 2, paragraph 4, of the Charter of the United Nations are interdependent in that if the use of force in a situation is unlawful – for whatever reason – the threat to use such force is also unlawful[72], therefore, the threat of using a cyber attack is related in its legitimacy to the legitimacy of the cyber attack itself. It is worth noting that cyber attacks that rise to the level of armed attack, although they justify the right of self-defense, this right is not absolute. The state's use of armed force in response to a cyber attack must comply not only with the Charter of the United Nations but also with the rules of customary international law, and what is included in the principles of the use of armed force, such as the principles of military necessity and the principle of proportionality in the use of armed force as well[73].

Among the requirements of the legality of resorting to force is the necessity to use force as a last resort when peaceful means such as diplomatic settlement are not feasible in achieving the general goal of the state[74]. Also, under the principle of proportionality, the use of force that is excessive in scope and intensity in relation to the actual or imminent danger of the military forces of another State is prohibited[75]. The question that arises here is: If cyber-attacks do not have massive effects on the level of armed conflict, can they be said to be unorganised? How does the affected country respond to such attacks?

To answer, it must be said that cyber-attacks that cannot be counted as using force are prohibited by Article (2/4) of the Charter of the United Nations, they can be considered similar to acts of political and economic pressure, and in this case they violate the (non-interference) rule contained in customary international law[76]. In this way, it can be said: Article (2 Fourth) of the Charter of the United Nations refers to the use of armed force, but the principle of (non-interference) applies to other forms of the use of force[77]. Hence, in order to respond to these attacks, the affected country, if it was able to get to know the identity of the perpetrators of

72.Oona Hathaway, op.cit, p.849.
73. R. Y. Jennings, The Caroline and Macleod Cases , 32 the American Journal of International law L.82,89, 1938.
74.Robert D. Slane, the Cost of Conflation: Preserving the Dualism of Jus ad Bellum and Jus in Bello in the Contemporary law of war, 34 the Yale Journal of International Law l.47, 2009.
75.General Assembly. A/RES/37/10, op. cit.
76.A. Randelzhofer, «Article 2(4)», in: Simma, B. (ed), The Charter of the United Nations: A commentary. Vol. 1, 2002, p. 118.
77.Charter of the United Nations, Articles: Article 1/35, Article 1/36, 39, 41, 42.

cyber attacks and attribute them to a particular country, can take the following methods:

1- Resorting to the Security Council based on Article (35) of the Charter of the United Nations, which states: "Every member of the United Nations may bring to the attention of the Security Council or the General Assembly any dispute or situation of the kind referred to in Article 34." The Security Council may recommend appropriate measures to resolve the conflict, and if the Security Council decides that the aforementioned conflict constitutes a threat to international peace and security, it may use its powers to issue recommendations and move to restore international peace and security. And if all these steps did not suffice, it may resort to his powers to use the land, sea and air forces"[78].

2- Resorting to the International Court of Justice in accordance with Article 34 of its Statute in order to hold the State responsible for the attacks and to obtain appropriate compensation for the damages arising from the cyber attack. Although the process of determining the balance of losses arising from a cyber attack is a very difficult process, due to the reluctance and secrecy of government financial institutions regarding the announcement of accurate information about losses[79]. Some of them argue that it is possible to resort to this court to obtain an advisory opinion requested by the main organs of the United Nations, on the legality of cyber attacks[80]. The advisory opinions of the Court, although not binding, help in the formation of a customary international norm[81].

3- The affected country may resort to countermeasures or reciprocal measures to respond to cyber attacks, provided that it does not report the armed attack[82]. This is according to the draft articles on State responsibility for Unlawful Acts of 2001, in particular articles (49-54) thereof [83].

78.Ali Qassemi and Victor Barin Jahar Bakhsh, Cyber Attacks and International Law, p. 129, a study published on (2/5/2012) on the following website: (last visit on 3/8/2016)
www.SID.ir/pdf
79.Charter of the United Nations, Article 96.
80.B. Conforti, The Law and Practice of the United Nations, Leiden Martins Nijhoff, 2005, p. 276.
81.The Charter of the United Nations, (Article 49 / I).
82.A. Randelzhofer, op.cit.p.118.
83.Michael N. Schmidt, War Using Communication Networks: Attacks on Computer Networks and the Law of War, International Review of the Red Cross, Selections from 2002 Issues, pp. 90-94.

Second: **Cyber Attacks Under the Law of War (Jus in Bello)**

Although a stand-alone cyber attack does not constitute an armed conflict, however, cyber attacks may be used during armed conflicts to respond to conventional provocations or to pave the way for a conventional attack in order to achieve military superiority and advantage[84]. The use of cyber attacks in armed conflict, as stated in the report of the International Committee of the Red Cross in 2011, must comply with all the principles and rules of international humanitarian law, as is the case, another means or method of warfare, whether new or old[85].

This is supported by what the International Court of Justice has indicated: "The principles and rules of international humanitarian law applicable in armed conflict apply to all forms of war and all types of weapons, including future ones"[86].

Accordingly, international humanitarian law or the law of war (Jus in Bello) applies to cyber attacks that occur during an ongoing armed conflict.

The experts at the United Nations also emphasized the applicability of established legal principles such as the principles of humanity, military necessity, proportionality in the use of force and the distinction between civilians and combatants to cyber attacks that occur during armed conflict[87].

First: **The Principle of Military Necessity**

The principle of military necessity relates to a specific military advantage that can be gained from a particular hostile action. While the issue of adapting the relationship between the principle of military necessity and armed conflict raises a jurisprudential dispute. A group of jurists believes that military necessity is one of the pillars of armed conflict and that a just war stems from a necessity that pushes to

84.International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Report of October 2011, available on the official website: www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st international-conference/31-int.conference-ihl-challenges-report-11-5-1-2-en.Pdf.

85.ICJ Nuclear weapons advisory opinion, op. cit., para 86.

86.Consider the report of government experts on developments in the field of information and telecommunications in the context of international security, Report No. A/70/174 July 22, 2015. Available on the official website: (last visit on 5/9/2016)
www.un.org/ga/search/viewdoc.asp?symbol=A/70/174,para.28.

87.Rebeca Grant, «In Determining Military Necessity and proportionality, The commander›s judgment is more critical than even, in search of lawful targets», Airforce magazine, Feb., 2003, p. 40.

wage it, which is military necessity, One of the supporters of this trend is the jurist de Forts, who went to say: "Military necessity continues to be a major element in combative operations"[88]. The jurist Henri Meyrowitz supported this trend and relied on the merits of the Brussels Peace Conference in 1874, in which the Russian delegation commented at the time: "Military necessity arises whenever the intention is established to achieve a legitimate military objective"[89] . As for the other group, on the exact opposite, they argued that military necessity is only an exception to the rule, and it cannot be resorted to, except in certain circumstances and according to specific conditions[90]. As for international law, the principle of military necessity has been referred to in several international instruments, including the preamble to the St. Petersburg Declaration of 1968, which states "... that the only legitimate objective that states should pursue during war is the weakening of the enemy's military forces. .." [91].

The Hague Convention of 1907 on the conduct of military operations affirmed that: "The High Contracting Parties consider that these provisions, which derive their formulation from the desire to alleviate the pain of war whenever military exigencies permit, serve as a general rule of conduct for belligerents, with each other and with the population"[92]. This convention stipulates in Article 23, paragraph (2/g) that "it is prohibited in particular... to destroy or seize the property of the enemy, unless the necessities of war inevitably require such destruction or seizure"[93].

In the same context, Article (52) of the Additional Protocol l of 1977 indicated in the second paragraph that: "Attacks shall be limited to military objectives only... whose total or partial destruction, capture or neutralization, in the circumstances

88.Henri Meyrowitz, «The principle of superfluous injury or unnecessary suffering - from declaration of st. Petersburg of 1868 to Additional protocol 1 of 1977», extract printofIRRC, no.299, March-April1994, p. 106.

89.Richard P. DimegLio, «The Evolution of the Just war tradition: Defining Jus Post bellum», Military Law Review, vol. 186, winter 2005, p. 120.

90 .International Committee of the Red Cross, "International Law Relating to the Conduct of Military Operations, Collection of the Hague Conventions and Certain Other Treaties," Geneva, second edition, September 2001, p. 169.

91 International Committee of the Red Cross, "International Law Relating to the Conduct of Military Operations, Set of Hague Conventions and Some Other Treaties," p. 13.

92.The previous source, p. 21.

93.International Committee of the Red Cross, "The Two Annexes, Additional Protocols to the Four Geneva Conventions of 1949, previous source, p. 43.

ruling at the time, offers a definite military advantage»[94]. On the occasion of its exposure to the project on international responsibility, the International Law Commission went on to say: "It must be recalled that resorting to military necessity is not permissible, unless the state is unable to achieve its legitimate military objectives except by taking urgent and necessary action to achieve that goal in order to protect the higher interests of the state"[95].

Based on the foregoing, it can be said that resorting to cyber attacks must be necessary to achieve the legitimate military objective. As for the issue of defining military targets and installations in cyberspace, it raises a broad challenge before the international community, because the installations that serve the military effort may at the same time serve the civil sector.

The failure to define regulatory standards for the use of cyberspace for offensive military purposes will mean the possibility of resorting to its use out of military necessity[96]. This challenge was pointed out by Rex Hughes, Director of the Cyber Innovation Network at the University of Cambridge, saying: «Digital attacks create a clear challenge to the application of the principle of military necessity, and to solve this dilemma, concerted efforts must be made between international law experts and electronic industries engineers to determine what can be described as a goal"[97].

Second: **The Principle of Proportionality in the Use of Armed Force**

One of the conditions for achieving the principle of proportionality in the use of force in armed conflict is what was stated in Additional Protocol I of 1977 in paragraph (5/b) of Article 51, as it states that: "An attack which is expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated"[98] (**98**). Article 57 of the same Protocol affirms: "An attack shall be canceled or suspended if it appears that the intended objective is not a military objective, or that it is covered by special protection, or that the attack may be expected to cause loss of life or injury to civilians, or Damage to civilian

94.UN, «Year book of the International Law Commission» vol. II, part 1, 1980, Article 3.
95.Ahmed Obais Nima Al-Fatlawi, previous source, pp. 630-631.
96.Rex Hughes, «A Treaty for cyber space», International Affairs Journal, vol. 86, No. 2, 2010, p. 537.
97.International Committee of the Red Cross, "Annexes" "The Two Additional Protocols to the Geneva Convention of 12 August 1949", previous source, p. 42.
98.International Committee of the Red Cross, "Annexes", "The Additional Protocols to the Geneva Convention of 12 August 1949", previous source, p. 42.

objects or causing a mixture of these losses or damages in an accidental manner that exceeds the direct military advantage expected from that attack[99].

Given the content of these articles, the application of the principle of proportionality requires military decision-makers to think carefully about potential civilian casualties or the destruction of civilian property in exchange for achieving military objectives . As for cyber-attacks, given the nature of the damage caused by these attacks, achieving the principle of proportionality poses a unique challenge to the international organization, because the effects of a cyber-attack are usually indirect[100]. For example, a cyber attack that stops the flow of information over the Internet may seem a mere inconvenience at first, but it will, for example, cripple the ability of hospitals to transmit vital information, and thus lead to loss of life and severe injuries[101]. In this regard, Shin went on to say: "The principle of proportionality can be applied to cyber-attacks...but we have to ask whether cyber-attacks can be considered an aggression no different from, for example, an attack using missiles"[102]. He adds, «The principle of proportionality in the use of cyber force is still ambiguous and needs answers, the most important of which is how to achieve proportionality in responding to cyber attacks»[103].

This was supported by Hughes, who went on to say: "If cyber-attacks are directed against an infrastructure of a dual-use (civil-military) and from a distance, it does not appear that the military advantage will be evident, which makes the application of the principle of proportionality during cyber-attacks extremely difficult"[104]. Achieving proportionality in cyber-attacks may be impossible, because information and communication technology is not equal in countries. Also, the victim country may be underdeveloped in terms of cyber-attack technology to respond to cyber-attacks directed against it[105], and the application of the principle of proportionality requires anticipating the likely consequences of hostile activity. and with regard to cyber-attacks and the ambiguity surrounding the type and severity of the effects of these attacks as a result of the infinity of the human mind, anticipating the likely

99.Ali Qasemi and Victor Barin Jahar Bakhsh, previous source, p. 134.
100.Oona Hathaway, op. cit., p. 851.
101.Shin Beomchul, , "The Cyber warfare and the Right of Self-Defense: legal perspectives and the case of the United States, IFANS, Vol. 19, No. 1, June 2011, p.118
102 ibid, p118.
103.Rex Hughes, op. cit., p. 538.
104.Greenberg, L. T., Information warfare and International Law, Mishawaka: National Defense University Press, 1998, p. 32.
105.Oona Hathaway, op.cit, p.851.

consequences of these attacks makes the application of this principle extremely difficult for military commanders, who in the context of cyber-attacks have to face more doubts and ambiguity about the legality of the attacks they will carry out[106].

Third: **The Principle of Distinction Between Civilians and Combatants**

This principle, which requires parties to a conflict to distinguish between civilians and combatants, and thus direct attacks on military targets rather than civilians, presents another challenge to international law. Under this principle, military commanders must use means capable of accurate targeting (not indiscriminate in effect), to distinguish between the civilian population and combatants, as well as between civilian objects and military objectives"[107].

The first paragraph of Article 50 of Additional Protocol I of 1977 defined civilians as: "persons who do not belong to the armed forces"[108]. This protocol defines military objectives in the second paragraph of Article 52, as it states: "Attacks are limited to military objectives only, and military objectives in relation to objects are limited to those that make an effective contribution to military action, whether that is by their nature, location, purpose or the use, of which, total or partial destruction, capture or disable it, in the circumstances prevailing at that time , brings a definite military advantage"[109]. This principle was confirmed in customary international law by the International Court of Justice in its advisory opinion on the legality of the threat or use of nuclear weapons, which stated in its decision: "States should not make civilians the object of attack, and accordingly they should not use weapons that do not discriminate between Civilian and military objectives" [110], and the Court went further, defining this principle as a peremptory norm by saying: "The principle of distinction is one of the main principles of international humanitarian law and one of the principles of customary international law that may not be violated"[111].

The International Criminal Tribunal for the former Yugoslavia confirmed this adaptation and considered the principle of distinction as one of the basic rules

106.International Committee of the Red Cross, "Annexes" Additional Protocols to the Geneva Convention of 12 August 1949, previous source, Article (48), p. 40.
107.Previous source, Article 50, pg. 40.
108.Previous source, Article 52, pg. 40.
109.ICJ Nuclear weapons advisory opinion. Op. cit, para 78.
110.Ibid, para 79.
111.ICTY , case II-95-11-R61, 8 March 1996, prosucort v. Matric, para 11.

of international humanitarian law and applicable to all international and non-international armed conflicts without exception[112].

As foe the cyber attacks, and according to this principle, the parties to the conflict are prohibited from launching attacks, directed against non-military targets, that intend or expected to cause death, injury, damage or destruction. Experts have confirmed in the Tallinn Guide in Article (38) of it, on what was stated in Article (52) of Additional Protocol I and they added a text to it saying: "Military targets may be computers, computer networks and cyber infrastructure"[113].

Applying the principle of distinction to cyber-attacks in some cases may be easy. For example, a cyber-attack, which targets the military air traffic control system and thus causes accidents in the transfer of military forces, would be lawful and not contrary to the principle of distinction[114]. As for the cyber attack on hospitals, museums, places of worship, the civilian banking sector, or the networks that run them, it is an unlawful attack as it clearly violates the principle of discrimination contained in international humanitarian law[115]. The application of the principle of distinction to cyber-attacks is very complex, due to the intertwining of the civil and military use of the same networks, as ninety-five percent (95%) of military communications use civilian networks at some levels, so it is possible that civilian networks can be attractive military targets[116].

According to the traditional understanding of dual-use objects, whenever a certain object is used for both civilian and military purposes, that object becomes a legitimate military target, if it makes an effective contribution to military action, or its destruction achieves a definite military advantage, provided that it takes into account the principle of proportionality in the harm caused to civilians[117].

112.Tallinn manual on the International Law Applicable to cyber warfare, op. cit., p. 125.
113.Michael N. Schmitt, wired warfare: Computer Network attack and the Jus in Bello, in computer network attack and International Law 187, 195 (Michael N. Schmitt 8 Brian To› Donnell eds., 2002).
114.Oona Hathaway, op. cit., p. 852.
115.Vida M. Antolin-Jenkins, Defining the parameters of cyberwar operations: Looking for law in all the wrong places? 51 Naval, REV, 132, 140, (2005).
116.Protection of Civilian Objects in International Humanitarian Law, 2008 Research published on the website: (last visit on 1/9/2016) http://www.mezan.org/uploads/files/8798.pdf
117.International Committee of the Red Cross, Report on International Humanitarian Law and Contemporary Armed Conflicts, 32nd International Conference of the Red Cross and Red Crescent (Force of Humanity), Geneva, Switzerland, 8-10 December 2015. Index No. 32IC/15XXX.

In the cyberspace, many objects that make up its infrastructure are dual-use, which makes them military targets not covered by protection, whether from kinetic or cyber attacks. However, this remains governed by the prohibition of indiscriminate attacks, the rules of proportionality, and the taking of possible precautions during the attack, and because civil and military electronic networks are highly interconnected, accidental civilian damage should be expected in most cases[118].

As for the most difficult challenge in applying the principle of distinction to the cyber-attacks is in distinguishing civilians from combatants, for several reasons including, the cyber-attack is often carried out by people who may be far from the site of the attack for distances that may exceed hundreds of miles, and this is what makes distinguishing between a fighter and a civilian extremely difficult if not impossible[119].

States may undermine the principle of distinction by using civilians to carry out cyber attacks, in doing so it places those civilians outside the protection they enjoy under international rules, for their participation in hostilities[120].

States do so either because those civilians possess technical expertise that governments do not possess or to conceal or deny their involvement in carrying out cyber attacks for fear of being subjected to counter-attacks or considering their use of such attacks as an illegal use of force[121].

Fourth: **Martinus Clause›s Principle**

The name «Martens» came after the Russian diplomat Fedor Fyodor Martens, one of Russia›s delegates to the Peace Conference in 1899, in which he stated: «In cases not covered by provisions, warring populations remain under the protection and authority of the principles of the law of nations as they came from traditions settled among civilized peoples, the laws of humanity, and the requirements of the common conscience"[122]. The condition is called the «alternative or precautionary

118.Ahmed Obais Nima Al-Fatlawi, previous source, pg. 632.
119.Oona Hathaway, op. cit., p. 854.
120.Jeffrey Carr, Inside Cyber Warfare 2010, p. 46.
121.Antonio Gessese, "The Martens Clouse: Half a loaf or simply pien the sky?" EJIL (2000), Vol. III, No. 1, p. 187-194.
122.International Committee of the Red Cross, "The Two Annexes, Additional Protocols to the Four Geneva Conventions of 1949, previous source, p. 118.

principle» because it is applied in the absence of a text protecting the person concerned, in relation to a case in which there is no explicit text. The importance of this principle is embodied in narrowing the scope of any interpretation, through which states deliberately legitimize the use of cyber-attacks unconditionally under the pretext of not agreeing on what restricts them under international humanitarian law, despite the latter's explicit prohibition of the use of methods and means of combat that do not discriminate between civilians and combatants in addition to causing excessively harmful injuries. The Martens clause confirms the authenticity of these principles, and therefore the legality of their use can never be invoked.

This condition was mentioned in the introduction to the Hague Conventions of 1899 and 1907 relating to the rules and customs of war on land, as well as in the Geneva Conventions of 1949, as it was included in Additional Protocol I of 1977, where the second paragraph of Article 1 states: "Civilians and combatants shall remain, in cases where no provision is made for them in this Protocol or any other international agreement, under the protection and authority of the principles of international law, as established by custom and the principles of humanity and the dictates of public conscience[123].

It was affirmed by the Second Additional Protocol of 1977 in its preamble where it stated: "In cases not covered by applicable laws, the human person remains under the protection of human principles and the dictates of the public conscience"[124].

In the context of cyber-attacks, Judge Shihab-al-Din stated in the advisory opinion issued by the international Court of Justice in 1996 regarding the legality of the threat and use of nuclear weapons, where he emphasized: "The Martens clause gives the authority to treat principles of humanitarian law and the dictates of public conscience as principles of international, leaving the precise content of the norm which principles of international law will require in light of changing circumstances, including changes in the means of warfare and the levels of appearance and tolerance of the international community"[125]. The Court also went in its advisory opinion that the Martens Clause "has proven to be an effective

123.The previous source, pg. 93.
124.ICJ Nuclear weapons advisory opinion, op. cit., Dissenting opinion of Judge Shahabuddeen , pp. 22-23.
125.ICJ Nuclear weapons Advisory opinion، op. cit.، Dissenting opinion of Judge Shah abuddeen، pp. 22-23.

means of countering the rapid development of military technology"[126], and on this basis the Court affirmed that the basic principles of humanitarian law remain applicable to all new weapons, including nuclear weapons, and stated that there are no State disputes it[127].

Concerning refuting the assertion that there is no legal regulation of cyber attacks, Erki Kodar, Undersecretary of Defense for Legal and Administrative Affairs in the Republic of Estonia and one of the authors of its constitution, goes to say: "The Martens principle indicates that in the absence of a clear mention in contemporary international agreements or By custom, the principles of limitation contained in the law of armed conflict will remain applicable in this case"[128].

Schmitt pointed out the applicability of this condition to cyber attacks by saying: "The Martens principle is the closest principle because it covers unregulated situations in international agreements, and this is only possible by resorting to customary international humanitarian law, that important source referred to in Article (38) of the Statute of the International Court of Justice"[129]. From the above it becomes clear that the absence of specific international rules – whether customary or treaty – regulating cyber attacks, does not mean implicitly acknowledging the permissibility or resorting to them, because they are inherently inconsistent with humanitarian laws and the dictates of the global public conscience in the event that they target facilities containing dangerous forces such as nuclear plants and oil pipelines Or civilian objects necessary for human survival, such as electricity and water networks[130]. In sum, the Martens clause is a safety valve that prevents states and other conflicting parties from using and developing new means of combat. It also cuts the way for states to evade responsibility on the pretext that there are no legal rules governing new means and methods that have not been addressed by international humanitarian law. And this is what can be relied upon in moving the international responsibility arising from cyber attacks, to fill the pretext that there are no explicit international provisions prohibiting their use.

126.ICJ Nuclear weapons advisory opinion, para 78.
127.Ibid, para 86.
128.Erki Kodar, Applying the law of armed conflict to cyber attacks: from the Martens clause to Additional protocol I", ENDC Proceeding, volume 15, 2012, p. 110.
129.Michael N. Schmitt, wired warfare: Computer Network attack and the Jus in Bello, op. cit., p. 369.
130.Ahmed Obais Nima Al-Fatlawi, previous source, pg. 634.

Countries and Their Responsibility for Cyber Attacks

Before the emergence of electronic means of communication (Digital Instructions), power and leadership belonged to those with military superiority and economic dominance. Today, however, electronic means of communication have radically changed this balance of power, and it has become one of the most important challenges facing world peace. The big issue has become to ensure that states do not use critical communications infrastructure as a weapon against civilians and civilian objects[131]. Information and communication technology poses an unprecedented challenge to countries regarding their national security. Under this development, individuals can thwart the authority, carry out cyber attacks that may paralyze the entire infrastructure, disrupt communications and cause massive damage to lives and property. Weaker countries with little technical expertise can pose a threat to the security of the largest countries[132].

The current basis of the communications network in cyberspace, Transmission Control Protocol and Internet Protocol, dates back to 1982, and this is an ancient communication system designed primarily for a small group of researchers and academics to exchange information among themselves in a low-risk environment in terms of exposure to breach. The risk of violation represents the core of the tracing of cyberspace attacks[133]. However, this is not the only problem. Rather, the system weaknesses pose doubly difficulties when considering the many software that exists today.

For example, identifying the source of an attack that appears is itself unreliable due to the possibility of manipulation, and therefore its denial[134], an example of which was the 1999 cyberattack against the US Department of Transportation via servers in Maryland, which is run by followers of the Falun Gong movement to show that these attacks were carried out by that movement to make it bear responsibility for the act, but the fact is that these attacks were aimed at sabotaging the servers of both Maryland and the US Department of Transportation, but that the United States of America has not been able to definitively determine who is

131.Ali Qassemi and Victor Barin Jahrbakhsh, previous source, p. 116.
132.The previous source, p. 116.
133.Lipson, H.F., Tracking and Tracing cyber-attacks: Technical challenges and Global policy issues, CERT Coordination center, 2002, p. 14.
134.Michael N. Schmitt, Heather A. Harrison and Thomas C. Wingfield, computers and war: Legal Battle space background paper prepared for informal high-level expert meeting on current challenges to international humanitarian law, Cambridge, June 25- 2004-27, p.99.

responsible for this until the present time[135]. In order to discuss the challenges of triggering international responsibility for cyber attacks, we will discuss the conditions that must be followed to trigger responsibility, which are:

First: **Attribution of the Cyber Attack**

Regarding international responsibility for cyber attacks, one of the conditions for establishing international responsibility in general is attributing the conduct to the state. As for cyber attacks, there are great difficulties in attributing them, due to the difficulty of tracing the source of sophisticated attacks carried out by professional hackers, whether they are working privately or supported by a state[136]. Attributing the cyber attack to the state is one of the basic elements, if not the only one, in building the legal system that deals with combating cyber attacks. Where the laws of war require the state to identify itself when attacking another state, despite the failure of states to comply with this tradition in most cases[137].

Responsibility is either direct or indirect. The state›s direct responsibility for cyber attacks arises in the event that any of its agencies, such as intelligence agencies, the army or internal security, for example, carry out cyber activities that lead to a breach of an international legal obligation. It does not matter then whether the action in question was carried out in application of express express instructions from the state or not, as long as that body acts in an official capacity as an instrument for expressing the will of the state[138]. Also, under the State Responsibility Draft Articles of 2001, persons and entities that are not state bodies, but carry a formal authorization under domestic law, when carrying out illegal cyber activities raise the responsibility of the state that has provided them with the authorization. For example, the government of a particular country providing a private company with an official authorization to carry out cyber attacks against another country, or providing a private entity with an official authority that authorizes it to carry out electronic operations to collect intelligence (Computer Network Exploitation), this raises the responsibility of the state in the event of these entities violate the rules

135.Mirage Thamer Ahmed, previous source, p. 128.

136.Scott J. Shackelford, State responsibility for cyber attacks: Competing standards for a growing problem, University of Cambridge, Dept of Politics and International Studies, Cambridge. U.K. 2009, p. 201.

137.Brenner S.W. & Grescenzi A.C., State-Sponsored crime: The futility of the Economic Espionage Act, Houston Journal International Law, 28, 2006, (pp 389-464), p. 398.

138.Abdul Karim Alwan, Mediator in Public International Law, House of Culture, Amman, 2010, p. 163.

of International law[139].

Here, a question comes to mind about individuals or groups who carry out cyber attacks against the informational or vital infrastructures of another state, and they are not state agencies or who have authorization from the state, so how can they be held accountable? In other words, how is the process of establishing the indirect state responsibility for the actions of these groups?

The answer lies in the extent of states' control over these groups or individuals and the type of link between them, as the indirect responsibility of the state is when the state supports armed groups to carry out cyber attacks outside its territory. As for what determines the state's responsibility for the actions of those groups is the amount of this support. We will show this in the light of the criteria of Overall Control and Effective Control.

1– According to the criterion of full control (Overall Control)

This criterion was first mentioned by the International Court of Justice in the Case of Military and Paramilitary Activities in or against Nicaragua in 1986, where it went to define the concept of full control as: "a criterion that specifies the attribution of the actions of individuals, armed groups or entities to the State itself" and indicated this by saying: "Such behavior must be under the strict control of the states and treat the other party, as if it were a subsidiary body. If this is proven, international responsibility can be triggered against the state for violations of individuals, armed groups or entities" [140].

In the Tadic case, the International Criminal Tribunal for the former Yugoslavia went on to determine the state's responsibility for the alleged violations committed by armed groups supported by it by saying: "… the state had a role in organizing and coordinating, as well as providing the armed group with support , which means that it has complete control over it, and what is issued by these armed groups, means that it is issued by the state itself"[141].

The jurists have gone to consider these groups by virtue of the apparatus of the state. For example, Derek Jinks went to say: "Although the state, as a general rule, cannot be held accountable for the actions of non-state actors, jurisprudence tried

139.Mirage Thamer Ahmed, a previous source, p. 130.
140.ICJ, Military and Parmilitary Activities in and against Nicaragua (Nicar v. U.S) op.cit, para.109
141.ICTY, Prosecutor v. Tadic, 1995, para 70

to address this dilemma, by counting the actions of these entities as actions issued by the state itself, according to the principle of (legal reality)[142]. In other words, consider them as state agencies by virtue of the legal de facto, which means the possibility of directing responsibility against the state, under penalty of exercising public authority, even if they are apparently entities that practice private behavior and are independent of the state"[143].

The adoption of the criterion of full control in deciding the responsibility of states for the actions of armed groups supported by them may be the most likely option with regard to cyber attacks, due to the difficulty of proving the state's involvment and the extent of its control over the perpetrators of cyber attacks with certainty, according to the effective control criterion that we will discuss later. Scott Shackelford supports this by saying: "If international law is to be satisfied with the application of one standard to cyber warfare, it is necessary that the standard of complete control be relied upon as part of a future international order in cyberspace[144].

2– According to the effective control criterion

This criterion was first addressed by the International Court of Justice, specifically in the aforementioned Nicaragua v. United States case[145], and the Court held that the criterion of effective operational control is the appropriate criterion for application, at least in relation to paramilitary forces[146]. The content of this criterion is that if the paramilitary or non–state actors depend in their actions to a large extent on a state and yet maintain their independence, then the actions of that group may be attributed to that state, provided that the link is proven. This is the view of the majority of jurists in the ruling of the International Court

142.The term de facto (De Facto) is a legal term that is usually used to deal with a legal act, as if it were a legal fact, without examining its legality. : http://legal-dictionary.thefreedictinary.com/de+facto

143.DerekJinks,»State Responsibility for the Acts of Private Armed Groups», Forthcoming, 4 CHICAGO J.INT›L L., 2003, p.1.

144.Scott Shackelford, op. cit., p. 203.

145.ICJ, Nicaragua Judgment, op. cit., para 115.

146.Capaldo G. Z., providing a right of Self-Defense Against Large Scale Attack by Irregular Forces: The Israeli-Hezbollah Conflict, Harvard International Law Journal Online, 48, 2007, (pp.101-112), p.104

of Justice in the case of Nicaragua v. the United States[147]. Similarly, the same criterion may apply to cyber attacks. A country may agree with a company or a citizen or a group of them to carry out cyber operations against another country, in addition to the state's assistance in financing skills and expertise, in order to plan to carry out cyber attacks, all of this leads to raising the responsibility of the state on the basis of effective control, which is not limited to mere material financing or equipment, but extends to participation in planning and supervision, although that group remains enjoying a high degree of independence from it[148].

In this case, the state's support for cyber-attacks does not raise its responsibility, unless its effective control over the perpetrators of the attacks is proven conclusively and leaves no room for doubt. Given the extreme technical difficulties in proving the identity of the source of cyber-attacks, this standard provides a free entry ticket to the countries supporting those attacks[149]. The adoption of the effective control criterion without any new techniques in tracking the sources of attacks may make the research into the responsibility of states for cyber attacks useless, and until that time, we can say: the loss or destruction of data may be sufficient to prove the state's control and take responsibility for it[150].

The International Court of Justice, in its most recent case concerning the specifying of international responsibility, regarding the Bosnian Genocide case[151], has gone to the adoption of the criterion of effective control, but in a more restrictive way. Judge Antonio Cassese criticized this ruling as «unrealistic» because it «requires a high level of proof» and this level is almost impossible to achieve in the context of cyber attacks[152]. Although, these two criteria provide some necessary support for determining the responsibility of the State for violations of international law through the use of cyber-attacks, relying on them entirely without an international convention dealing with these attacks may be unrealistic[153]due to the difficulty

147.R. J. P. Pronk. ICTY Issues final judgment against Dusan Tadic in first international war crimes tribunal since world war II, Human brief, center for human rights and humanitarian law, 1997.

148.Antonio Cassese, "The Martens Clouse: Half a loaf or simply pien the sky?" EJIL (2000), Vol. III, No. 1, p. 652.

149.Scott Shackelford, op. cit., p. 202.

150.Ibid, p.202.

151.ICJ, Case of: Bosnia and Herzegovina. V. Serbia and Montenegro, 2007.

152.C. Tosh, Genocide Acquittal provokes legal Debate, Institute for War and Peace Reporting, March 2, 2007.

153. 93(3)H. F. Lipson, Tracking and Tracing cyber-attacks: Technical challenges and Global policy issues, CERT Coordination center, p.3.

of identifying the attacker to take measures necessary to trigger international responsibility against his own state and international criminal responsibility against the perpetrator of the attacks himself, as well as the difficulty of curbing any tendencies to commit similar attacks in the future, because these attacks take on the vast field of cyberspace because they are immaterial behaviors that cannot be proven by normal methods[154].

Second: **Unlawful Cyber Attack**

The second condition for the establishment of State responsibility is the unlawful and harmful act. In the context of cyber-attacks, they do not constitute an unlawful act except in the following cases:

1- Violation of the principles of the Charter of the United Nations, such as the attack amounting to the use of force through electronic means if it is attributed to a specific country.

2- Violation of international obligations imposed by international humanitarian law, such as targeting civilian objects with cyber attacks, such as information systems that control the supply of electrical energy, if assigned to a specific country.

3- Violation of international rules in peacetime and outside the context of armed conflict, such as violating the principle of non-interference in the affairs of a particular state[155].

On the other hand, a cyber-attack is illegal under international law if it causes damage to the target country, which entitles it to resort to countermeasures, including electronic ones, to stop the attacking country from violating the rules of international law, provided that the attacking country is warned in advance of taking such measures[156]. Except in the case of necessity, where the affected state may take countermeasures without prior notice in order to preserve its rights[157]. Countermeasures are intended to compel the attacking State to stop its breach of international rules and, therefore, such measures must not conflict with:

"1- An obligation to refrain from the use or threat of force in accordance with

154.See Ahmed Obeis Nima Al-Fatlawi, previous source, pp. 638-639.

155.Mirage Thamer Ahmed, previous source, p. 128.

156.The General Assembly of the United Nations, "Report of the International Law Commission on the work of its fifty-third session", previous source, Article (43).

157.The previous source, Article (52/F2) Also see: Tallinn manual on the international law applicable to cyber warfare, op. cit , Chapter I, section II, rule 6.

the Charter of the United Nations and for such countermeasures to not reach the level of armed attack.

2- Obligations to protect basic human rights.

3- Obligations of a humanitarian nature that prevent reprisals.

4- All other obligations in conformity with general standards of international law[158].

The countermeasures must be proportional to the harmful act, i.e., the reaction of the affected state be appropriate to the wrongful act so as not to violate the principle of proportionality[159]. For example, when country B carries out cyber attacks against the power plant in the dam of country A to force the latter to increase the flow of water to the river that passes through the two countries, country A response with cyber operations against the irrigation control systems of country country B is a lawful countermeasure, i.e., it is proportional to the attack[160]. Emphasizing this, the arbitration court, in the case of interpreting the air agreement between France and the United States of America, went on to say: "...the countermeasures are aimed at consolidating the pillars of legitimacy between the concerned parties"[161]. But if the effects of the cyber attack are of such gravity and severity that they reach the level of an armed attack, then the target country may resort to the right of legitimate defense under Article 51 of the Charter of the United Nations.

158.The previous source, a. NS. NS. D / F1 / M 50.

159.The General Assembly of the United Nations, "Report of the International Law Commission on the Work of its Fifty-Third Session", previous source, Article (51) Also considers:
Tallinn manual on the international law applicable to cyber warfare, op. cit, Chapter I, section II, rule 9.

160.Tallinn manual on the international law applicable to cyber warfare, op.cit, p.37.

161. Decision of the Court of Arbitration between France and the United States of America on December 9, 1987.

Conclusion

Cyber attacks are one of the most important contemporary challenges facing the international community, because of their repercussions on the national security of countries and a threat to international peace and security. But it is still a modern concept that there is no international agreement on its definition, which leads to the difficulty of adapting it and determining international responsibility for it.

-The comparative advantage of cyber attacks lies in their low costs and ease of resorting to them, as they do not require crowds of military fighters, thousands of weapons, and means such as conventional armed conflicts. Rather it is sufficient to implement them by a person or a small group who have experience and skill in cyber technology and software and computer systems vulnerabilities in order to be used against a country or other countries. But this feature turns into a source of great concern if we look at the effects of these attacks and their consequences on the civilian population and the environment if they were carried out on a nuclear facility or energy sources such as the electricity and water network.

With regard to cyber attacks that occur during the conventional armed conflict, international jurists have unanimously agreed that they are subject to international humanitarian law; However, the greatest challenge are those attacks that occur in peacetime and the extent to which they can be considered as armed attacks that raise the right of legitimate defence, and when to be cosidered as a violation of the principle of «non-interference» that only allows the use of countermeasures and other peaceful means in confronting them.

- Determining the state›s responsibility for cyber attacks is characterized by great difficulties, due to the difficulty of attributing the attack to the state, because cyber-attackers often use hide softwear, which leads to difficulty or even impossibility to reach the source of the attack in most cases. And even if the source of the attack is reached, it is very difficult to prove its connection with the state, especially in the event that the source is a non-governmental entity, which leads to a double difficulty in proving the state's support for that entity and the amount of this support.

Despite the fact that cyber-attacks are a relatively recent concept and are developing very rapidly, they do not occur in a legal vacuum. It can be based on the opinions and decisions of the International Court of Justice, such as its opinion

on the legality of the threat or use of nuclear weapons, its judgment in the case of military and paramilitary activities in or against Nicaragua, and the case of the genocide in Bosnia, as can also be based on the decision of the International Criminal Tribunal for the former Yugoslavia.

- There are international efforts made in order to regulate cyber activities, such as the Budapest Convention, the Tallinn Guide, and resolutions issued by the United Nations, and there are laws, although they were prior to the emergence of cyber attacks, but they regulate the means and tools that may be used in their implementation, which can be referred to. However, these efforts did not rise to the level of comprehensive organization of these attacks.

-The relationship between law and technology is a reciprocal relationship. Various technological developments require keeping pace with legal legislation, either at the internal level of the state or at the international level. However, cyber activities (especially cyber attack) lack strict legal frameworks to deal with them. Contemporary international laws and regulations, though applicable to cyber attacks, but they do not cover all forms and challenges of cyber attacks. Hence, international agreements must be concluded to regulate these attacks in detail, in order to protect the international community from severe humanitarian consequences, whether bloody, physical or environmental.

-The process of developing a comprehensive regulation of this dangerous phenomenon is characterized by various difficulties, because the international interests of the great powers stand in the way, such as the difficulties faced by the international community when drafting a convention on nuclear weapons and the controversy over restricting them or banning their use entirely.