مجلة الشرق الأوسط للنشر العلمي
المجلد (٥) العدد (١)
الإصدار الرابع عشر
٢٠٢٢ (٣٩٠-٣٧١)

The applicability of the rules of international humanitarian law to cyber-attacks in war

Joman Rabah Al-Khateeb
Email: Joman.alkhateeb2000@hotmail.com
Under the supervision of:
Dr. Hamza Abu Issa
& Dr.Mahmoud Abu Turabi.

Published on: 11 May 2022

Abstract

This article illustrated a new method of war that began to appear on the scene of conflicts in the international community in light of the spread of cyberspace, which added to wars new war tools based on the exploitation of technological progress and the great development in the wide use of the Internet and social media and the use of these tools in a military framework capable of causing damage that may be stronger and more affecting the infrastructure of countries involved in armed conflicts and may exceed that effect to cause significant damage civilians and everything related to civilian life in all respects. Because of the significant impact of cyber-attacks, it has been problematic in the applicability of the rules of international humanitarian law to such cyber-attacks. In this article, she addressed the concept of these cyber-attacks and some of their methods used in conflicts, as well as their impact on the field nature of war and civilians, as demonstrated by the legitimacy of cyber targets and what civilian data are targeted from cyber operations, and in conclusion reviewed the applicability of the principles of international humanitarian law to those attacks and the mandatory extent of Tallinn evidence and how it can influence the course of use of cyber-attacks to ensure that civilians are not harmed or at least minimize Civilian damage in all its forms, whether direct human or vital targets for infrastructure that serves civilians.

Keywords: International Humanitarian Law, Tallinn Guide, International Armed Conflicts, Non-International Armed Conflicts, Cyber Attacks, Cyber Warfare.

* Introduction

* Boot

International humanitarian law has regulated the rules of war methods and the means used to carry them out, it has restricted those methods by identifying the types of legitimate and illegal weapons, the systems of their methods of use and the methods and principles that must be followed by the parties to conflicts, and the technical development of the world has been followed by methods of war that have become clearly used during conflicts, and a new method of war has emerged: cyber-attacks.

* Search goal

This study aims scientifically to examine the scope of the application of the rules of international humanitarian law to cyber-attacks in war and to properly classify them within those rules.

In practice, this study aims to enrich human rights activists and jurists from this modern method, which has become used by wars and armed conflicts, and the lack of a clear text to regulate it.

* The importance of article

The issue of violations of international humanitarian law is of paramount importance as it leads to the loss of many lives and landmarks in the country and this applies to cyber wars as in conventional wars, and therefore this subject is of interest to jurists and humanitarians, as it contributes to the disclosure of the findings of international efforts in laying the legal basics of cyber operations accompanying the wars.

* The problem of article

Coinciding with field military operations in armed conflicts, cyber operations have emerged, but there has been no change in the rules of international humanitarian law in the four conventions or in the additional protocols, and here is the problem in the extent to which traditional rules apply to armed conflicts accompanied by cyber operations.

*** Problem elements**

1- What are cyber-attacks?

2- Is there a difference between cyber warfare and cyber-attacks?

3- What does the civilian nature of cyberspace entail?

4- What are the legitimate objectives of cyber-attacks?

5- How mandatory is Talin evidence?

*** Article methodology**

This study is based on two approaches to article, we have used the analytical approach due to the ambiguity of this subject in terms of the applicability of traditional rules of international humanitarian law to cyber-attacks in war, which is the majority of the topics of the study, and the descriptive approach to the study of trials that have taken place and the development of logical interpretations based on evidence and evidence.

*** Previous studies**

1- Saleh Haidar Abdul Wahid, Cyber Space Wars; Study in Its Concept, Characteristics and Ways to Confront It, Master's Thesis, Middle East University, 2021

This study aimed at articling the wars of cyberspace and its characteristics but was based on the Charter of the United Nations and articled its provisions and based its methodology on the historical approach and comparative approach in addition to the descriptive analytical approach.

2- Dr. Rola Hatit, Cyber: Hidden War in the Dark Zone, Lebanon.

This study aimed at defining cyber wars, their origin, their classification among the means of combat and their change in the concepts of conflict-force, but did not look at the applicability of the rules of international humanitarian law to these wars.

But we differ from this study, which expanded the concept of cyberspace, while in our study we will highlight the problem of cyberattacks in war only within the scope of international humanitarian law.

*** Terminologies**

1- International humanitarian law is a set of rules that limit the effects of armed conflicts and its humanitarian motives protect individuals who are not involved in or stop combat operations, and establish restrictions that restrict the methods used during the war, and have other names such as "law of war", "law of armed conflict".

2- *International* armed conflicts are armed conflicts between two states and more.

3- *Non-international armed conflicts* are armed conflicts that are within the borders of the state itself between armed and organized groups such as civil war, with the exception of internal unrest and tensions.

4- *Tallinn Guide: An academic study by nato's Center of Excellence for Collaborative Cyber Defense examined the application of fair war declaration rules and the rules of* international human law to cyberwarfare.

5- Civilian objectives are targets that are not used for military purposes during armed conflicts.

1- What cyber-attacks.

Many countries around the world are developing and using Internet and computer skills as tools for attack, defense, intelligence operations and psychological warfare, and according to media reports and international reports the United States, Britain, South Korea and France have established armed forces dedicated to cyber warfare or informatics, combining military acumen with technical skills to enable them to cause losses or defend and repel attacks, and on the other hand, the use of the Internet has become increasingly An effective tool for armed groups to wage wars and cyber-attacks, they have found an effective way to fight in cyberspace to recruit soldiers through it and achieve their military wishes.

A- The concept of cyber attacks

Cyber-attacks are attacks on computer networks and are a war operation used by parties to the conflict to carry out action that influences.

In the enemy system and determine its own information, which affects the security of his country, i.e. it consists of cyber operations by a particular state or non-governmental group and is in the form of offensive or defensive operations, aimed at causing military or civilian damage or both against the opposing party, and this is done by entering illegal means with the intention of deleting, modifying or encrypting data or disrupting political, civil or military services or spreading malware This is done with computers, websites or technical organizations. [1]

[1] Michael N. Schmitt, Computer network attack and the use of force in international law- Thoughts on a normative framework, Columbia journal of transnational law, 1998– 1999, p. 890

International humanitarian law defined attacks in Article 49 of Protocol I: "Offensive and defensive acts of violence against the adversary", and based on this definition it included the broad meaning of attacks and therefore it is agreed that cyber-attacks that cause injury to individuals or cause any material damage so-called attacks, such as cyber-attacks causing airport closures, suspension of emergency flights, or cutting off electricity to medical conditions in health centers and causing deaths From the patients.

- Cyber-attacks in international and non-international armed conflicts

International humanitarian law is represented by the four Geneva Conventions and the first Geneva Convention was established in 1864 and the fourth in 1949 and its additional protocols, and these agreements provide for the protection of fundamental human rights in the situation of war, the methods and means to be followed during armed conflicts, but the differences the world has witnessed between traditional armed conflicts and cyber armed conflicts have had a clear impact in terms of the perception developed by these conventions and charters of armed conflicts and their means and means. Its effects, however, continue to be based on clear and valid foundations for armed conflicts marred by cyber-attacks.

The ICRC has emphasized the applicability of international humanitarian law to cyber-attacks during armed conflicts and its importance in reducing and organizing such attacks, just as it has organized various new or old armed conflicts, although the cyberspace field of armed conflicts is new, but the rules of aerospace, maritime and land also apply to it, while it is a man-made area.

There is no logical legal basis that distinguishes conventional attacks and cyber-attacks in war with regard to the application of the rules of international humanitarian law to it in international armed conflict, where it is clear that cyber-attacks in war require that they be accompanied by international combat operations on the ground and the use of violence and force that have been banned in those rules and conventions.

As for cyber-attacks in non-international armed conflict, it is complex, unlike international armed conflict, and the cases of violence have been classified Anson-international armed conflict on the basis of two criteria in accordance with common Article III:-

- To show a certain level of organization among the participating parties.
- Violence reaches a certain level of intensity.

Since internal unrest and tensions are not called an international armed conflict, non-international cyber-attacks and attacks do not amount to the use required to classify such attacks as non-international armed conflict.

According to the Former Yugoslav Court, the conflict is classified as non-international based on the standard of organization, as the command structure of armed groups, the mechanisms followed and the rules and the ability of these groups to obtain weapons, military exercises and logistical support must be available, and in the case of cyber-attacks it is difficult to prove or detect such organization among thousands of websites and persons used as a human shield behind the devices that are hacked to carry out these cyber-attacks associated with field operations. Armed. [2]

The Court also decided with regard to the standard and severity of violence, taking into account the number and severity of confrontations, the types of combat means and tools used, the number of munitions, the number of individuals involved in the conflict and the extent of the destruction caused by the conflict, both human and civilian objects, and therefore cyber-attacks face the ambiguity of legal rules in international humanitarian law, whether written or customary, as the prohibition of types of cyber weapons that go beyond what is It is also allowed and has not specified its permissible severity either.[3]

International humanitarian law merely foresees the development of combat methods and the development of new methods, stating in Article 36 of the Additional Protocol I of the Geneva Conventions: "When studying, developing, acquiring, acquiring a new weapon, a war tool or a method of war, any high-ranking contracting party is obliged to verify

[2] Tadic case IT-94-IT- 7 May 1997

[3] Diya Haradinaj, T-84-04-ITJudgement, 3 April 2008, paragraph 49, Boskowski's case, IT–82-04-T، 10 July 2008, paragraph 177

whether this is in any case prohibited or in some cases under this annex, the Protocol or any other rule of international law that adheres to It has that high contracting party," the law has established a general framework governing the use of such attacks.

- Methods of Cyber attacks

It is difficult to direct the precise and proportionate force of cyber-attacks because of the high accuracy required in the electronic means used in such attacks, since the target could be military, industrial or civilian.[4]

The methods used in cyber-attacks are based on targeted data collection, modification, sabotage or control of different systems for change or destruction of their work, and cyber-attacks on various sectors such as the industrial or political sector or the infrastructure of countries to create electronic disability by affecting the national security of countries or by influencing their basic services, and cyber-offensive and defensive methods continue to evolve due to the development of technology in the world, targeting These methods are often accurate, radio communication stations and radar systems of all kinds, and try to detect electro-optical guidance systems, and weapons are directed through systems that analyze signals and waves that are reflected from the pulses of wave frequencies of electromagnetic fields.[5]

Access to other party systems indicates that conflict is critical and may be accessed by telephone, Internet services or wireless networks, but there are specific situations that require proximity to those systems through the human element, such as the use of spies in data targeting locations, such as system operators, suppliers or computer chip manufacturers, or the encryption of certain files with the ability to penetrate the firewalls of discount systems.

Certain international reports may be intercepted, changed and dangerous cases caused by this change, and may be in targeting certain software with viruses hidden inside them, whether in infrastructure or in state systems, and the methods of such attacks may vary in the form of

[4] Helge Janicke - Wikipedia , Cyber warfare: Issues and challenges , 2015 , p.10

[5] Abdul Ghaffar, Faisal, Electronic Warfare, p. 28, Janadriyah Publishing and Distribution, Jordan, 2015.

sabotage on the[6] government's internet networks or by spreading cyber false news or spying on adversary systems to identify confidential data affecting his country's security, such as Russian cyber-attacks on Estonia. In 2007, it targeted the websites of Estonian organizations, including parliament, radio, banks, ministries and newspapers.

A report has been published by the International Committee of the Red Cross stating that it is in the interests of states to assess the legality of the methods and means of war represented by new weapons, including the compatibility of the conduct of the armed forces of those countries on the basis of international obligations, and a commitment to Article 36 of the Additional Protocol I, which obliged all parties to armed conflict to take into account the new weapons they use or [7]deploy, as The global recognition was based on the fact that the right of parties to all armed conflicts to choose the methods and means of combat operations is restricted by specific restrictions and not by absolute rights.[8]

B- The realistic application of cyber-attacks.

Cyber warfare may seem "new," but the truth is the opposite, it has been part of the geostrategic landscape for at least 15 years, and possibly as many as 30, starting in the United States at the outbreak of the Civil War in 1861, when signal staff were eavesdropping on telegraph lines to get data of interest to them from the adversary, and fire-correcting ships were used by radios in 1904 by two Japanese ships that attacked a Russian naval base. Arthur and there are reports that President Ronald Reagan agreed in 1982 to introduce secret malware into supervisory control and data acquisition (SCADA),a system that led toa large-scale explosion and major damage to the Soviet gas pipeline.[9]

As for the recent attacks, the cyber-attack associated with the crisis between Russia and Ukraine, where Russian cyber-attacks were launched

[6] Peter Hruza, Jiri Cerny , Cyber warfare , Czech , 2017 , p.157

[7] A report by the Red Cross "What restrictions does the law of war impose on cyber-attacks?" https://2u.pw/h2kmq

[8] Melzer, Nils, International Humanitarian Law: A Comprehensive Introduction, p.101, 2016.

[9] Krepinevich, Andrew, Cyber Warfare a "Nuclear Option"? , p.36,CSBA , 2012 ,

on websites for Ukrainian detergents and institutions, such as banks, electricity companies and ministries, and malware was used (PETYA)

- The military use of cyber operations and its impact on the field nature of cyberspace

We have mentioned the widespread use of technology in both armed conflicts and defensive and offensive operations, and military operations are not an exception of this kind nor are they limited to field operations, but technology now controls the management of military forces, where control of logistics depends on modern technologies, as military forces work to develop their field weapons by introducing modern technologies on them, which increases their strength and reduces the resulting losses. For their use, the military also uses the necessary techniques to coordinate their movements through communication networks that expand coverage of the field of armed conflict and war.

The U.S. Department of Defense has defined "cyberspace" as the use of information technology and electromagnetic spectrum for storage, modification and exchange of data through network systems and infrastructure, and the military operates on the definition of the Department of Defense in the Cyberspace to carry out its military operations, The civilian basic of the Internet and radios used in military communications and operations.

One of the most notable examples is the Falklands War between Argentina and Britain in 1982, where English forces created a new radio station that broadcasts daily transmissions to Argentina in Spanish, which is used in Argentina, to create a bad psychology for the people and undermine their confidence in their armed forces, and in the same way argentine forces broadcast a daily radio addressed to the English military, broadcasting propaganda in English for them and old English village music to make them interesting to return home.[10]

These cyber-attacks may be military plans, as happened in 2007 in the suspected nuclear reactor carried out by the Israeli enemy's air force on

[10] Al-Basili, Jassim, Electronic Warfare: Its Foundations and Impact in Wars, p. 166, Arab Foundation for Studies and Publishing, 1989.

a Syrian site simultaneously for the Israeli enemy to also carry out cyber-attacks on radars and communications in the Ministry of Defense and communication systems at civilian military airports, resulting in complete failure of operation.

Therefore, countries are working to establish special cyber units in their armed forces to strengthen their defensive and offensive forces cyber, support them with the latest technology and recruit the most skilled pirates and programmers in their forces, due to the growing concern arising from the misuse of modern technologies by terrorists or extremist groups and incitement to cyber-attacks, and the Security Council warned of this and pointed out the need to share appropriate training of communication networks and maintain the protection of the military sectors and civilian whether public or private from those cyber-attacks [11]

- Distinguishing between cyber-attacks and cyber warfare

Cyber-attacks are part of cyber warfare, i.e. cyber-attacks that amount to material effects in armed conflicts and are equivalent to the results of conventional attacks are called cyber warfare, while cyber operations that harm adversary states, whether in peace or in war, are called cyber-attacks, whether they cause material effects on lives, but only because of cyber operations, i.e. not accompanied by field work, or by jamming computer systems for military, field or field purposes. Penetrate them.

The term cyber-attacks contain a broader and more general concept of cyber warfare, and cyber-attacks must be associated with armed conflicts and wars to be brought within the scope of international humanitarian law, it is possible to have such cyber-attacks, but within peace situations the rules of international humanitarian law do not apply to them.

Cyber warfare is also an armed conflict that finds its field on land and on cyberspace, while cyber-attacks involve only cyberspace.

In terms of motives, the motives of cyber-attacks must be politically motivated solely on information and regulations, namely, disrupting official

[11] Security Council Resolution 2341 of 2017 at its 7882 sessions, held on February 13/ February 2017

state websites, obstructing basic services, stealing and hacking confidential data and other possibilities, the most prominent example of which [12]is the motives of the Russian-Georgian war following the secession of Ossetia from Georgia in 2008, and the in production of the Electronic Communication System (IT). The Georgia forces, one day before the start of hostilities, weakened the air defenses of the Georgia forces, and the owner of those attacks damaged the media and transportation infrastructure as a result of those cyber-attacks.

Cyber-attacks must bear some independent features in order to live up to cyber warfare and achieve in a strategic political context, in which the American political scientist Colin Gray argued that even if cyber-attacks have independent features, they still have to occur in a political and strategic context commensurate with their call for war, i.e. it is the real cyber warfare that is based on effective command systems, control and communication between different forces, and their field includes various fields. Land, air, sea and cyberspace. [13]

2- Framing cyber-attacks within international humanitarian law

With the development of modern technology and technologies, the methods and means used by armed conflicts have become new, and in conjunction with that development, the international humanitarian law system is working to develop the legal organization of these cyber armed conflicts, where armed conflicts are taking cyberspace as a field, which has had to be framed cyber-attacks in armed conflicts within international humanitarian law in accordance with the treaties, conventions and protocols concerned, which have already been mentioned.

A- direct problems of cyber operations within international humanitarian law

In the absence of any explicit legal provision providing for cyber-attacks and their regulations, a range of problems have been formed regarding the nature and elements of these attacks and the determination of their legal scope within the rules and

[12] Saad, Mohammed, Cyber Warfare: Its tools are fueled by its losses, p.11, electronically published, 2020.

[13] Schnouf, zineb, Cyber Warfare in the Digital Age: Post-Klazovic Wars, p. 93, Algerian Journal of Security and Development, Algeria, 2020.

principles of international humanitarian law, those rules relating to the provision of the legality or illegality of such attacks and the statement of what cyber elements may be targeted in such attacks.

- The legitimacy of targets by cyber-attacks

The legitimacy of cyber-attacks lies in targeting legitimate targets, distinguishing what should not be targeted, and adhering to all the rules of international humanitarian law to take into account the negative effects of such attacks and not exposing civilian targets to any risks.

The principle of discrimination has not been limited to specific types of attacks or weapons, but is applied and adhered to in various types of attacks, including cyber-attacks, and the St. Petersburg Declaration of 1868 stated: "The only legitimate purpose targeted by states during the war should be to weaken the enemy military forces, and it is sufficient to isolate as many men as possible from fighting," as well as the text of the first additional protocol to protect civilians from the dangers[14] of war. For combat attacks except civilians involved in combat, they are excluded from this protection, and in doing so the International Court of Justice has gone on to recognize the mandatory applicability of the principles and established rules of international humanitarian law to various forms of war and to all types of weapons, including what will be developed in the future.[15]

It is difficult to identify civilians involved in cyber-attacks non-participants because most individuals now use computer systems and are familiar with them, and here it is necessary to identify the cyber attacker and not the devices that were used for cyber-attacks, because the cyber attacker may threaten the civilian to hack and use it as a "human shield", here the cyber attacker is the legitimate target of attacks and not the civilian subject to the cyber attacker, it is possible that the cyber attacker penetrates civilian electronic devices to carry out his tasks Through it, here is the legitimate target of the attacks and is also responsible for the damage to civilian devices when targeted, and

[14] Lülf, Charlotte: Modern Technologies and Targeting Under International Humanitarian Law ,P7,, Germany,2013.

[15] Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflicts, p. 4, 2019.

when determining criminal liability it is possible to rely on the country where the electronic device that started the cyber-attack and identify the person who used this device and linked to the target directly attacked and the precise geographical location of it.

Technical engineers play a crucial role in establishing electronic systems that handle cyber-attacks, and their role does not exempt them from punishment as they are legitimate targets of legal accountability for their illegal use of technical military advantage.

- What is civil data and civilian objects in cyber operations

International humanitarian law defines civilian objects as those that are not military targets, and the same applies to civilian data as objects unless this status is lost and used for military purposes, and these civilian data include various types such as biometric medical data, tax record data, bank statements, electoral register data, electricity and communications networks and customer data in various companies and government ministries, i.e., all data that are aside. Fundamental to the aspects of civil life, and with its great importance, it is increasingly important to protect it because tampering with it, sabotage or modifying it leads to paralysis in the work of civil and government systems.[16]

The problem lies in determining whether civilian data are dual, i.e., the armed forces use civilian networks and data that are originally used for civilian purposes, but the ICRC has authorized the targeting of these objects and considers them military rather than civilian, but with the requirement that the principle of proportionality be achieved where the expected collateral damage to cyber-attacks on these civilian objects is commensurate with the expected military advantage.

If there is a doubt about the classification of objects and statements whether they are civilian or military, what the first additional protocol has to do is applied, since it is obligatory to assume that the eye is a civilian eye and is not used militarily because of the uncertainty that has occurred. [17]

[16] Rule 9 of customary international humanitarian law

[17] Article 52/3 of The First Additional Protocol :" If there is doubt as to whether an eye is usually

B- The application of international humanitarian law to cyber-attacks

Once the concept of cyber-attacks and their framing are established within the rules of international humanitarian law, they will be shown within the consistency of the principles of international humanitarian law, their applicability to cyber-attacks and the mandatory extent of the Tallinn Guide.

- The basic principles of international humanitarian law apply to cyber-attacks.

The importance of the general principles of international humanitarian law, which worked to regulate armed conflicts and their means and methods and included all possible developments, namely the military necessity that the intended targets of cyber-attacks must be targeted for the necessity to defeat the enemy and for military purposes and failure to accurately determine the criteria to be observed for the use of information technology for offensive military purposes will lead to the possibility of resorting to Its use on the grounds of military necessity, which is evident in the statements exchanged by the United States of America and Russia, and the principle of discrimination in relation to military attacks stipulates that civilian data or information systems not used for military purposes cannot be targeted, as stipulated in article 48 of the First Additional Protocol of 1977 [18] and Article 51/2 of it, [19] as stated in Article 52 of the same Protocol. In customary international humanitarian law,

devoted to civilian purposes such as a place of worship, a house, any other dwelling or school, it is used to make an effective contribution to military action, it is assumed that it is not used either."

[18] " "The parties to the conflict distinguish between the civilian population and combatants and civilian objects and military targets, thereby directing their operations against military targets only, in order to ensure respect and protection of the civilian population and civilian objects."

[19] " The civilian population as such, as well as civilian persons, may not be the subject of attack and violence or threats aimed primarily at broadcasting Panic among the civilian population"

the[20]end of the principle of proportionality, which makes it work to make the proportion of damage caused by cyber-attacks proportional to the proportion of military advantage required and provided for in customary international humanitarian law, but the problem lies in the fact that technology systems and[21] military devices are connected to commercial and civilian systems. Relying entirely or in part on them, which makes it difficult to launch cyber-attacks on military targets and limit their effects to those targets, experts in international humanitarian law Rex and Shin stressed this: “If cyber-attacks are directed against infrastructure used for dual civilian-military use and remotely, it does not appear that the concrete and direct military advantage will be clear, making the application of the principle of proportionality during cyber-attacks something It is recognized that the [22]use of civilian objects for military purposes makes them a military target and therefore is not protected under international human law.

In an advisory opinion, the International Court of Justice also recognized the establishment of international humanitarian law on two basic principles, and given the mandatorily of these principles, they apply entirely to cyber-attacks:-

- States must never make civilians the target of attack and must therefore not use weapons that cannot distinguish between civilian and military targets.
- The use of weapons that cause undue pain is prohibited, and this principle is contained in the Hague Regulations on the Laws and Customs of Land War 1907 that "the right of the warring parties to choose the means and methods of combat is not an unlimited right."

[20] Rule 7 of customary international humanitarian law : "At all times, the parties to the conflict distinguish between civilian objects and military objectives. Attacks are directed only at military targets, and may not be directed at civilian dignitaries.".

[21] Rule 14 of customary international humanitarian law :" An attack that may be expected to accidentally cause civilian casualties or injuries, damage to civilian objects, or a combination of such losses and damage, is prohibited and is excessive in overcoming the expected tangible and direct military advantage.”

[22] Shine, Beomchul, p. 118

It is worth mentioning the most important principles relating to cyber-attacks, which is the Martins clause stipulated in the Fourth Hague Convention in its preamble, and in the preamble to The Second Additional Protocol, and in the First Additional Protocol, and this requirement provides for the absence of a certain rule of law, the combatants remain in the protection of customary international humanitarian law and its general principles and what is required by the public [23]conscience, In this regard, the International Court of Justice went on to emphasize the importance of the Martens clause as the effective means of confronting the technological development of military methods in armed conflicts. [24]

One of the principles that measure cyber-attacks in wars is the principle of refraining from the use of force, which is stipulated in the Charter of the United Nations, which stipulates that states refrain from using force to threaten or against the territorial integrity or political independence of any state or in any way that does not conform to the objectives of the United Nations, and according to this prohibition the right of defense of the states that have been attacked and that right is stipulated in the same [25]Charter, and has This right was confirmed by the U.S. Department of Defense in 2011, where it affirmed the right of defense of the United States of America against cyber-attacks and justified the use of appropriate force

[23] Article 1/2 of The First Additional Protocol :" Civilians and combatants in cases not provided for in this annex , protocol or any other international agreement, remain under the protection of"

[24] Dozwald, Louise, Blinding Weapons, Geneva, 1993.

[25] Article2/4 of the Charter of the United Nations :" In their international relations, all members of the Commission refrain from threatening or using force against the territorial integrity or political independence of any state or any other aspect. Disagrees with the purposes of the United Nations.

for this attack in order to achieve justice. [26]

- Mandatory Talin Guide

Cyber-attacks targeting Estonia's cyber infrastructure in 2007 and the 2008 cyber-attacks against Georgia during the armed conflict with Russia led NATO to respond to cyber-attacks, establishing the Center for Collaborative Cyber Defense for Excellence and evaluating the extent to which the rules of law apply to cyber-attacks, and subsequently, in 2013, a Talin guide was established, which provided for Applying international law to cyber wars.

These experts launched two versions of this guide, the first in 2013, consisting of 95 legal rules, and stressed the seriousness of cyber-attacks that violate the prohibition of the use of force in international law and the right of States to defend themselves mentioned earlier in this article, which occur in armed conflicts and are applied to them international humanitarian law, and the second version in 2017 consisted of 154 legal rules and He stressed the legality of piracy and cyber-attacks that are at peace and when cyber-attacks are considered a violation of international law, and has based evidence on the rules of international humanitarian law and defined cyber-attacks as cyber operations, whether offensive or defensive, expected to cause injuries or civilian casualties, damage or destruction of civilian objects, [27] One of the most prominent things that is stated in Talin evidence is that civilian objects cannot be considered the target

[26] Article 51 of the Charter of Nations United:" There is nothing in this Charter that weakens or detracts from the natural right of States, individually or in groups, to defend themselves if an armed force attacks a member of the United Nations until the Security Council takes the necessary measures to maintain peace and international security, and measures taken by members using the right of self-defense are immediately communicated to the Council, and those measures in no way affect the Council -- under its authority and continuing responsibilities under the provisions of this Charter -- the right to take any action in any at some point he sees the need to take action to keep the peace for international security or to restore it to normal".

[27] Farghaly, Muhammad Allam, Digital Violence Latest New War Trends, Humanist Magazine, Issue 59, 2018.

of cyber-attacks, and therefore such attacks aimed at destroying civilian systems and infrastructure cannot be directed unless they are identified as military targets, [28] and Koh considered that cyber-hybrids are a use of force, if they compare the most those attacks ,The actual use of force is equal to or close to it.[29]

Tallinn's evidence has not been used as a mandatory document for states, but at least it is considered by NATO members as a moral document regulating the use of cyber-attacks during armed conflicts.[30]

*** Conclusion**

We are witnessing a frantic acceleration in the huge amount of scientific and technical development, and this development has covered all areas of life and became the biggest dominant in all sectors, and it is not strange to see the greater impact of this development on the nature of war conflicts and its greater exploitation of all parties and even seeking to develop it further and the frantic race to develop the capabilities of military personnel to gain military superiority, that the use of cyberspace in war conflicts gave the opportunity for the conflicting parties to impose their control It has even gone beyond its legal limits and expanded the amount of damage to include civilians and service facilities that they benefit from without taking into account the civil and humanitarian rights imposed by international laws in regional and international conflicts, and the rules of international humanitarian law must be amended to comply with this development clearly and explicitly, but this does not mean mandatory its basic principles on these attacks, namely discrimination, necessity, proportionality and applicability to cyber-attacks. It has also become clear to us that every cyber war involves cyber-attacks, but not every Cyber-attack is considered a cyber-war, and states are trying to make all efforts to ensure an atmosphere of protection from such attacks.

*** Recommendations**

1- A law must be established to regulate cyber-attacks in conflict to

[28] Article 37 of the Tallinn Guide .

[29] Koh, H., International Law in Cyberspace, Harvard International Law Journal, Online Volume54,2012, p.4

[30] Khalifa, Ihab, PowerNoلElectronic How countries can manage their affairs in the age of the Internet, p. 166, Arab Publishing and Distribution, Egypt, 2017.

ensure the safety of civilians and the infrastructure they serve

2- And find solutions to fix the legal loopholes used in cyber-attacks.

3- International efforts to find defensive cyber systems to deter illegal cyber-attacks directed at countries that affect their national security

4- Work to ensure the mandatory Talin guide.

5- Affirming the comprehensiveness of the principles of international humanitarian law to include cyber-attacks in armed conflicts.

6- Clarify the Martens clause in a broader way and explicitly enter it into the provisions of the rules on international humanitarian law.

*** References**

Abdul Ghaffar, Faisal, Electronic Warfare, Janadriyah Publishing and Distribution, Jordan, 2015.

Al-Basili, Jassim, Electronic Warfare: Its Foundations and Impact in Wars, Arab Foundation for Studies and Publishing, 1989.

Khalifa, Ihab, Electronic Power: How Countries Can Manage Their Affairs in the Age of the Internet, Arab Publishing and Distribution, Egypt, 2017.

Saad, Mohammed, Cyber Warfare: Its fuel tools and losses, electronically published, 2020.

Dozwald, Louise, Blinding Weapons, Geneva, 1993.

Farghaly, Mohamed, Digital Violence Latest Trends of New Wars, Al-Ihsani Magazine, Issue 59, 2018.

Schnouf, Zainab, Cyber Warfare in the Digital Age: Post-Klazovic Wars, Algerian Journal of Security and Development, Algeria, 2020.

A report by the Red Cross, "What restrictions does the law of war impose on cyber-attacks" to see: https://2u.pw/h2kmq

Decisions of the former Yugoslav Court

Decisions of the International Court of Justice

Red Cross Report, "International Humanitarian Law and Cyber Operations during Armed Conflict, 2019.

Security Council Resolution 2341 of 2017 at its 7882 meeting on February 13, 2017.

Additional Protocol II to the Geneva Conventions, 1977.

Charter of the United Nations

Customary International Humanitarian Law

Protocol I to the Geneva Conventions, 1977.

Tallinn Guide

Krepinevich, Andrew, Cyber Warfare a “Nuclear Option”? , CSBA .2012

Lülf ,Charlotte: Modern Technologies and Targeting Under International Humanitarian Law,Germany,2013

Melzer, Nils, International Humanitarian Law: A Comprehensive Introduction. 2016

Shine, Beomchul.

Helge Janicke , Cyber warfare: Issues and challenges , 2015

Koh, H., International Law in Cyberspace, Harvard International Law Journal, Online Volume54, 2012.

Michael N. Schmitt, Computer network attack and the use of force in international law- Thoughts on a normative framework, Columbia journal of transnational law, 1998– 1999.

Petr Hruza, Jiri Cerny , Cyber warfare , Czech , 2017