

The Compliance of Cyber warfare with the Principle of Distinction in the Light of International Humanitarian Law



Soltani Smail

University of Larbi Ben Mhidi in Oum El Bouaghi (Algeria)

soltani.smail@univ-oeb.dz

Submission date: 22/03/2025 Acceptance date: 30/05/2025 Publication date: 04/06/2025

Abstract:

This research dealt with the subject of cyber warfare compliance with the principle of discrimination in accordance with international humanitarian law. It aims to shed light on the definition of cyber warfare, distinguishing it from similar terms, the possibility of availability of the conditions of armed conflict in cyber warfare, and its compliance with the principle of distinction. Based on the descriptive, analytical and deductive approach. The research concluded that cyber warfare can be considered an international armed conflict if the conditions of the armed conflict are met. Cyberwarfare is often consistent with the principle of distinction in IHL, but it may not meet the requirement of discrimination in certain cases. This is due to the specificity of the cyberspace in which cyberwarfare takes place, which is fundamentally different from the traditional domain of classic international armed conflicts. Cyberwarfare is a fundamental challenge facing international humanitarian law, which requires adapting its rules to cyber warfare in cyberspace.

Key words: Cyber warfare; Principle of distinction; International Humanitarian Law; Cyberspace; Compliance.

الملخص: تناول هذا البحث موضوع امتثال الحرب السيبرانية لمبدأ التمييز وفقا للقانون الدولي الإنساني. يهدف إلى إلقاء الضوء على تعريف الحرب السيبرانية، تمييزها عما يشابهها من مصطلحات، إمكانية توافر شروط النزاع المسلح في الحرب السيبرانية، وامتثالها لمبدأ التمييز. بالاعتماد على المنهج الوصفي والتحليلي والاستنباطي. خلص البحث إلى أن الحرب السيبرانية يمكن أن تعتبر نزاعا مسلحا دوليا إذا تحققت فيها شروط النزاع المسلح. الحرب السيبرانية تتسق مع مبدأ التمييز في القانون الدولي الإنساني في غالب الأحيان، لكنها قد لا تستوفي شرط التمييز في حالات معينة. وذلك يرجع إلى خصوصية الفضاء السيبراني والإلكتروني الذي ترتكب فيه الحرب السيبرانية، الذي يختلف اختلافا جوهريا عن المجال التقليدي للنزاعات المسلحة الدولية الكلاسيكية. تعتبر الحروب السيبرانية تحديا أساسيا يواجه القانون الدولي الإنساني، يستوجب تكيف قواعده مع الحروب السيبرانية في الفضاء الإلكتروني.

الكلمات المفتاحية: الحرب السيبرانية؛ مبدأ التمييز؛ القانون الدولي الإنساني؛ الفضاء السيبراني؛ الإمتثال.

Introduction

Technological development has played a crucial role in bringing about a digital revolution over the last three decades, where communications have become remote between the parties of the international community in general. The exchange of information between various digital media such as desktop computers and smart phone devices has also made the process of family and professional interconnection easy, allowing the transfer of various information instantly, inexpensive, reliable, and decentralized.

This stimulating and attractive electronic situation, which individuals cannot do without in any way, has made it a desirable and palatable electronic space by countries because it is inexpensive, easy to master, and at the same time, a space to carry out cyber operations and attacks against vital targets that may be physical, kinetic, or may be against base facilities directly related to civilian life. The thing that happened in 1982, when the Soviet gas pipelines were blown up in the Siberian region, by planting a bomb related to the computer systems that run this station, which resulted in significant material losses. This incident was considered as the first offensive cyber-attack at the time. (Romala, Volume 7, Issue 2, 2021,)

Currently, it is very easy to use the Internet as a digital medium to carry out cyber attacks, which can lead to a total or partial harm to the vital interests of States, such as those related to civilians or national security, including disabling nuclear power plants, damaging the air defense systems of the armed forces, or those of civil aviation authorities. This situation poses challenges for states in two key areas. First, there is the legal adaptation of cyberattacks and the question of whether they qualify as armed conflicts under international humanitarian law. Second, the methods and means used in these attacks differ significantly from those of traditional armed conflicts, whether international or non-international. Additionally, there is the issue of whether cyberattacks can be classified as armed conflicts and thereby subjected to the law of armed conflict through appropriate legal adaptation.

The importance lies in examining the topic of cyber warfare and its compliance with the principle of discrimination in accordance with international humanitarian law, as it is one of the topics that need to clarify its nature, means, and methods of committing it, as well as examining the issue of its consistency with the principle of discrimination from the perspective of international humanitarian law.

This article aims to shed light on cyber wars as an emerging type of conflict that meets the conditions of armed conflict in accordance with international humanitarian law, their compliance with the principle of

discrimination or not, and the susceptibility of the law of armed conflict to contain these wars, as it is the legal framework regulating armed conflicts.

In order to achieve the above-mentioned objectives, the researcher followed the descriptive and analytical approach of the legal texts related to the law of armed conflict, and the deductive approach in studying cyberwarfare and its response to the conditions of armed conflict and the applicability of international humanitarian law to it.

The research paper addresses a key issue: **How does International Humanitarian Law apply to cyberattacks as international armed conflicts, and to what extent do they comply with the principle of distinction?**

To answer this question, the study follows the following structure: The concept of cyber attacks (the first requirement). The extent to which the conditions of armed conflict are met in cyberattacks (the second requirement). Cyberattacks comply with the principle of distinction (the third requirement).

The first requirement: the concept of cyber warfare

We must address the concept of cyberattacks, the means used in cyberattacks, and distinguish them from other similar terms according to the following:

Section I: Definition of Cyberwarfare:

Many perspectives have sought to define cyberattacks to clarify their meaning and scope, facilitating their legal adaptation and application under the law of armed conflict. One such definition states that a cyberattack is "an intentional attempt to maliciously access personal information or sensitive data, or to steal money from bank accounts without authorization" (Shulman, 2025). Additionally, cyberattacks can cause total or partial disruption, or varying degrees of damage, to essential services such as transportation, electricity, the Internet, and critical infrastructure vital to civilian life (Shulman, 2025).

Cyberwarfare is also defined as the sum of the actions taken by the parties to the armed conflict in order to obtain tangible advantages for their benefit towards their opponents in cyberspace, by nagging, disrupting, damaging, or penetrating computers or Internet networks. (Shuweirb Jilali, 2023, p. 160) In the same context, Michael Smith defined cyberattacks as those actions taken by the State in order to attack information systems and, thus, influence and harm them, while, at the same time, defend the attacking State's information systems. This fact can lead to offensive or defensive armed conflicts, resulting in damages to civilians and their property, and the destruction of vital facilities as determined by international humanitarian law. (Najib, 2021, p. 222)

In addition, cyberwarfare is defined as a term derived from the Greek word **Kybernetes** in the sense of remote command and control without direct

human interaction, and it means remote control of animals and machines without direct contact. It also takes the meaning of attacking the information in the possession of the opponent with the intention of damaging him, his property, or his strategic weapons. (Al-Zayat, 2017, p. 62)

In fact, most of the definitions of cyber warfare are consistent in their general meaning, which is to target digital systems, computer devices, by digital means of communication, in order to disrupt, destroy, or access sensitive information of the other party, so that these programs are controlled and made to work in a counterproductive manner for the benefit of the perpetrator against the interest of the State that owns the information system. (Haidara, 2017, p. 186)

In addition to the definitions mentioned above, others have defined cyberattacks as the use of the electromagnetic or electronic spectrum for the purpose of storing, changing and exchanging information and data on infrastructures connected to systems that it controls. Another doctrine (Al-Fatlawi, 2016, p. 616) has also defined them as activities carried out by a State through which it wishes to access and hack computers and related networks owned by another State in order to cause significant damage or disable them. (Yahya Mufrah Al-Zahrani .. , 2017, , p. 235) A NATO experts' team also touched on the concept of cyber warfare and formulated it in the Tallinn Manual, stating that it is the entirety of cyber operations, whether defensive or offensive ,that are expected to cause significant damage and death to civilians, damage to objects by destroying them, or cause serious damage to them. ("NATO», 2013)

Professor Michael N. Schmitt has defined Cyber attacks that are activities carried out by the State for the purpose of attacking the enemy's information systems, with the intention of causing serious damage to them and influencing them in a way that allows the attacking State to confront and defend its information systems. (Michael N. Schmitt, 1998-1999, p. 890) in a similar definition to the previous one of the jurist (Michael Schmidt), both (Richard Clark and Robert Knackie) tried to provide a definition of electronic warfare to the effect that a group of actions initiated by one country against another by resorting to penetrating computers and all digital networks connected to them for the purpose of disrupting or causing severe damage to them that prevents them from functioning in a correct and proper manner. (Yahya Mufrah Al-Zahrani, , January 2016, p. 67)

In the context of our definitions of cyberattacks, the International Committee of the Red Cross (ICRC) has provided a definition of cyberwarfare as an intentional and deliberate process of activities carried out by the State against computer-connected systems, or digital networks to disrupt, destroy, or corrupt them so that these attacks result in a major breach of electronic property, prevent the opposing party from using this data belonging to it, or impose

censorship that prevents access to digital platforms, or use that information as it wants, or in a reverse manner. (Herbert Lin, Summer 2012, p. 522)

In light of what precedes, we can define these cyber attacks as attacks carried out in a purely digital environment using digital tools and Internet networks, by an attacking party in which official data and sensitive information are the subject of cyber attacks with the aim of their acquisition or theft, disrupting their work, partially or completely damaging them, damaging civilian or military facilities, or killing or injuring civilians as a result of those attacks.

Section Two: Means of Cyber Attacks:

Researchers and technicians agree that cyberattacks, carried out in the digital space, use modern methods commensurate with the nature of the digital environment. This is in contrast to classical wars in which armies and means of warfare, represented by land, air and sea weapons, are used in the specific battlefield on land, air or sea. Consequently, these cyberattacks are likely to be ambiguous in their objectives, unspecified in scope, taking place in a purely electronic and digital space, transcending international geographical borders. (Yahya Yassin Saud, , 2018, p. 84) One of them adds that cyber wars are distinguished from other classical wars, as they are based on means and weapons of an electronic nature, or operate in an electronic environment that inevitably leads to extremely destructive and dangerous effects on a large scale. (Amr Reda Bayoumi, ,2002, p. 25) The definition developed by the United Nations Conventional Weapons Commission in 1968 , regarding non-conventional weapons, refers to atomic explosion weapons, weapons made of a substance with radioactivity, chemical and biological lethal weapons and any other type of weapons.....). (Omar bin Abdullah bin Said Al-Balushi, 2007, p. 15)

The means used in cyber-attacks lie in seven (07) types of cyber-attacks: (See the link: (Seen on 02/03/2025), 2025)

- A) **Espionage:** It is intended by the State Party to monitor the adversary and hunts for the opportunity to steal secrets by means of botnets, resort to hacking into computer systems, and access sensitive information.
- B) **Sabotage:** The state seeks to sabotage the facilities and vital interests of the opposing party through careful sorting of sensitive information intended to be stolen and destroyed or through the exploitation of personnel belonging to the other party.
- C) **Denial of Service Attacks:** (Laurent Gisel, 2018) These attacks cause a continuous refusal to access the website by making fake requests that force it to deal with them, so that it disrupts the processes and procedures that enable civilians and military personnel to access sensitive websites.

- D) **Electric Power Grid:** This method of attack allows the disruption of all targeted vital systems, which may amount to physical harm, rendering services and communications unusable and unusable.
- E) **Propaganda Attacks:** This type of attack aims to control the ideas of those people who live in a targetable country, so that they promote lies and misinformation that lead them to lose confidence in their country, or conspire against it with them.
- F) **Economic Tension:** In this method, attackers target the digital networks of economic institutions through the computer in certain platforms such as financial markets, payment systems, banks, or deny customers access to their money. (Laurent Gisel, 2018 , pp. 23-24)
- G) **Sudden Attacks:** This type of attack is based on the method of surprise in the implementation of cyber attacks at a time that the opponent cannot predict, which weakens his defensive capabilities, and paves the way for the attacker to initiate a real physical attack, taking advantage of the situation that the opposing party has reached.

Reports indicate that there are recent attacks, which the media has responded to, for example, the Stuxnet virus, a worm that attacked the Iranian nuclear program, and caused serious damage to it that amounted to an inability to manufacture. (Laurent Gisel, 2018 , pp. 23-24) Estonia was also subjected to a cyber-attack in 2007, when it changed the location of a statue related to the Russian Federation, from the center of the capital Tallinn to a military cemetery along the city, after which Estonia was subjected to a huge number of cyber-attacks, where government sites, such as banks, suffered from a very slow processing of data ,often ending up refusing service, which lead to the disruption of that service. (Laurent Gisel, 2018 , pp. 23-24)

Section Three: Distinction Between Cyber Warfare and Similar Terms:

There are many terms that benefit the meaning of cyber attacks, or present an imminent convergence of these terms with the term cyber warfare, and this is what we will study according to the following detail:

1/Cyber Warfare and Electronic Warfare:

It is inevitable that cyberwarfare and electronic warfare are fairly close to the point that it is difficult to determine the discrepancy between them, (Salih Erdem Erol, 2018, pp. 1-10), (Haig., p. 23) but the fact is that there is a fundamental difference between the two terms. Electronic warfare boils down to the use of the electromagnetic spectrum in order to disrupt devices, various control systems, especially the communications device, jamming radars, and protecting the armed forces from attacks on three levels : electronic jamming,

electronic hacking , and electronic protection (Salih Erdem Erol, 2018, pp. 1-10). As for cyber warfare, it means attacks carried out against computer networks and digital systems, where information is stolen or disrupted using certain means such as hacking, malware, attacks to stop and disconnect the service, and cyber espionage.

2/Cyber Attacks:

As already mentioned, intentional and deliberate attack using subversive activities with the intention of achieving divergent economic, social, political, or any other objectives. (U.S. Army Training & Doctrine Command, 2006) An intentional action aimed at altering, disrupting, or destroying hostile computer networks or programs in or through them. (Gervais M. , Cyber Attacks and the Laws of War, October 2011)

3/Cyberspace:

Cyberspace is the domain and arena on which cyber warfare is conducted, and it is also the fifth domain of warfare, after land, sea, air and space. (Domain, 2010) Richard Clarke also defines cyberspace as the sum of the world's computer networks and those connected to the Internet, and other networks that are not connected to the Internet. (R Clarke, 2010, pp. 1-2) Some jurisprudence goes on to say that both cyberspace and the electromagnetic spectrum, in the military sub-civilian field of it, are one coherent and continuous environment, on which modern warfare is based, and that any bet to win these wars is contingent on the concomitance of cyberwarfare as a space for the electromagnetic spectrum formed from frequencies ranging from zero (0) to infinity , which consists of 26 bands containing all wavelengths of frequencies (such as commercial radio and television, microwave and radar). (R Clarke, 2010, p. 2)

The Second Requirement: The Availability of the Conditions of Armed Conflict in Cyber Warfare

International humanitarian law requires certain conditions that indicate the existence of an armed conflict, whether international or non-international, that calls for the beginning of the applicability of international humanitarian law, without the need to know the causes of armed conflict and the circumstances that led to its outbreak in reality. From this standpoint, we address the conditions for the existence of an armed conflict (Section I), and then show the extent to which these conditions apply to cyber warfare and its compliance with these conditions (Section II).

Section I: Conditions for the Availability of an International Armed Conflict:

The Geneva Conventions of 1949 provide that any international armed conflict between two High Contracting Parties to the Conventions, or any occupation, however partial, shall be deemed to be an international armed conflict whether recognized by the Parties or not, even if it meets with no resistance from the other Party. (convention, 1949, p. art 2), (Cross, March 2008, p. 1) So that the practical effect is the decisive factor in determining the beginning of the hostilities between the two parties, and the beginning of the application of international humanitarian law, without taking into account the declaration of a state of war or not. (Schindler, 1979, p. 131.), (Association, 2010, p. 2) In this regard, it is necessary to separate the law of war (*Jus in bello*) and (*Jus ad bellum*), because the existence of an armed conflict is related to the beginning of the application of international humanitarian law on the ground, and not to discuss the legality of the use of force based on the Charter of the United Nations. (Greenwood, , 'International Humanitarian Laws of War': Revised Report for the Centennial Commemoration of the First Hague Peace Conference 1899 ',), e: Reports and, , The Hague, 2000,), (François Bugnion, September 2002,)

The existence of an actual armed conflict also requires the participation of the armed forces of at least one party in hostilities, taking into account what is stipulated in Article II (M2), paragraph (1). (David, 2012, p. 122.)

The intensity of violence used between the parties of an armed conflict do not require a specific limit, as a general principle, for the beginning of the application of international humanitarian law. It is sufficient that there is a dispute between two High Contracting Parties, which leads to resort to the use of armed forces, and the capture of a member of the hostile armed forces in accordance with the text of Article IV (4) of the Third Geneva Convention 1949, (Pictet (ed.), 1958, p. 2021) even if the other Party does not recognize the state of war. Because linking the existence of an armed conflict to the necessity of achieving a certain level of violence ultimately leads to the incompatibility of the purpose of imposing protection under the Geneva Conventions of 1949, as well as the possibility of the parties evading the application of international humanitarian law on the pretext that the condition that requires its application is not met, and can miss the protection of a captured prisoner, and his inability to enjoy the legal status of a prisoner of war as stipulated in the Third Geneva Convention. (Hans-Peter Gasser, 1993, pp. pp. 510, 511), (David, 2012, p. 122)

In contrast to what was stated in the first opinion not to require a certain level of intensity of violence, to say that there is an armed conflict, an exception, as part of the jurisprudence believes that the description of an armed conflict can only be achieved if a certain level of intensity is available. (International Law

Association, 2010, pp. 32-33) States always resort to characterizing the individual and non-continuous use of armed force as an armed incident or provocation that does not meet a certain intensity of violence to avoid acknowledging the existence of an armed conflict situation that requires the application of international humanitarian law. (Greenwood, Scope of Application of Humanitarian Law, 2008, p. 48)

Based on the aforementioned points, recognizing a minimum threshold of intensity as a criterion for classifying a conflict as an armed conflict could undermine the application of international humanitarian law. This approach would allow conflicting parties to define the nature of the conflict based on their own interests rather than objective facts. Moreover, it would contradict the fundamental purpose of the Geneva Conventions, which is to ensure the protection of those affected by hostilities. Additionally, reliance on the law governing the use of force (*jus ad bellum*) cannot provide adequate protection, as it primarily establishes a legal framework for assessing the legitimacy of force between states rather than offering protective rules for individuals affected by armed conflict. (United Nations Charter, p. art 51)

On this basis, the absence of a specific threshold for the level of violence between parties to an armed conflict appears to support the objective of ensuring protection for civilians and civilian objects. This principle is reflected in Article 2 of the 1949 Geneva Conventions, which does not impose a particular intensity requirement for a confrontation to be classified as an armed conflict. By refraining from setting such a limit, the Geneva Conventions reinforce their primary purpose: safeguarding those affected by hostilities regardless of the conflict's scale.

Section Two: Applicability of an Armed Conflict to Cyberwarfare:

According to Common Article 2 of the Geneva Conventions, an international armed conflict is defined as any dispute that results in the use of armed force between states. However, applying this criterion to cyber warfare presents challenges, as cyber operations are non-kinetic and do not involve the conventional use of physical weapons. Nevertheless, dismissing cyber warfare as "unarmed" would be illogical, given that its consequences can be widespread, violent, destructive, and even fatal. Cyberattacks have the potential to disrupt essential infrastructure, cause economic devastation, and even result in loss of life, making them a significant aspect of modern warfare that may necessitate legal adaptation within international humanitarian law. (Michael Schmitt, 2012,, pp. 250-251) Any cyber operation described as offensive can be adapted as armed in the manner adopted by Protocol I. (Protocol I, p. 48(1)) For example, in 2010, a cyber attack called "Stuxnet" occurred on the nuclear power plant targeting the Iranian nuclear program, causing severe and verified damage, which means that cyber warfare responds to this standard and achieves material

damage. (Micheal N Schmitt, (2011), pp. 89, 92–94) Cyber operations that disrupt a specific program of a state are considered attacks, even in the absence of physical damage. This perspective is supported by the International Committee of the Red Cross (ICRC), which states that an attack includes cyber operations that lead to the disruption of a computer system or software, particularly when such disruptions significantly impact a state's vital and fundamental interests, such as transportation, energy, and the economy. This interpretation highlights the evolving nature of warfare, where the effects of cyberattacks can be just as consequential as traditional armed attacks, necessitating their consideration under international humanitarian law. (Micheal N Schmitt, (2011), p. 252)

In addition to being armed, cyber warfare must be of an international nature in order to achieve the legal characterization of an international armed conflict. Based on this proposition, all acts carried out by the State from its governmental bodies, or those that are under the auspices of the State, whether committed by groups or individuals of an international character, are also considered against the vital interests of a second State. (ILC), (Responsibility, p. art4(2)) As confirmed by the ICTY in the Tadić case, persons exercising their functions under the authority of or in partnership with the armed forces, or under their authority, are de facto organs of the State. (para, (15 July 1999)) By analogy, all cyberattacks carried out by these people, as I mentioned earlier, are considered as acts of the state by virtue of law. Those actions committed by individuals or entities in an isolated from any framing of the state, and do not meet this requirement are not considered international cyber attacks, nor constitute a non-international armed conflict because individuals do not constitute an organized armed group. (Articles on State Responsibility, , p. art 5)

The Third Requirement: Cyber Attacks Comply with the Principle of Discrimination:

We will address the content of the principle of discrimination from the perspective of international humanitarian law (Section I), and then turn to discuss the extent to which cyberwarfare complies with the principle of discrimination (Section II).

Section I: The content of the principle of discrimination in international humanitarian law:

The principle of distinction requires that the parties of the armed conflict commit to limiting combat and hostile operations to targeting purely military objectives only, which necessarily weaken the enemy's combat power, such as attacks between combatants and military objectives. At the same time, they should not target civilians and civilian objects. (Oona A. Hathaway R. C., 2012,

pp. 851-853) The principle of distinction finds its basis in the text of Article 48 of Additional Protocol I to the Geneva Conventions of 1949, “The Parties of an armed conflict shall act to distinguish between the civilian population and combatants and between civilian and military targets, and shall commit themselves to directing their military operations against military targets only. (Yves Sandoz, 1987, pp. 1410–1439)” Moreover, the ICRC went on to emphasize that this principle - the distinction between combatants and civilians - is one of the fundamental principles in the laws and customs of war inspired by the principles of customary international law. (Yves Sandoz, 1987, p. 598) In its Advisory Opinion on the Legality of the Threat of nuclear weapons, the International Court of Justice also affirmed that the principle of distinction in any targeting and attack is a fundamental principle of international humanitarian law. (Justice, 1996, pp. 226, 257) Even States who did not adhere to Protocol I shall refrain from placing military personnel or equipment in the vicinity of civilian sites and targets because this is a flagrant violation of the content of this principle and entails responsibility for the party that violates the content of the principle. (Oona A. Hathaway R. C., 2012, p. 1873)

Section Two: Cyberwarfare Compliance with the Principle of Discrimination:

International humanitarian law requires that armed conflicts comply with the principle of discrimination, so that they can be subjected to it, and monitor the extent to which they achieve and take into account the target groups of armed conflicts. The law allows attacking military targets but not civilian installations, and it also legalizes targeting combatants but no other civilians who have nothing to do with armed conflict. (protocol I, p. art 48), (ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts,, November 2019, p. 486) The principle of distinction requires that cyber attacks must be consistent with the content of the principle, in order to ensure the protection of civilians and civilian objects, so that attacks must not be indiscriminate and do not achieve the principle of distinction. (ICRC, The Principle of Distinction, Cyber Operations during Armed Conflict, ,, March 2023, pp. 1-3)The ability of cyberwarfare to meet this requirement is questioned during international armed conflicts. According to international humanitarian law, the fighter is characterized by organization and responsibility, which is achieved only by armed forces endowed with significant cyber capabilities in

carrying out cyber attacks that fall within the scope of international armed conflicts. Piracy activists (Gervais M. , *Cyber Attacks and the Laws of War* (, October 1, 2011, p. 34) also raise the problem of not being considered legitimate combatants as determined by international humanitarian law. At that time, they are not combatants, and at the same time, they are not legally protected civilians. (Protocol I, pp. 47-51(3))

Cyber attacks are characterized by rapid implementation without warning, and they also raise questions regarding the principle of discrimination. One quotes the case of a cyber-attack in which the attacker is forced to use a computer of a civilian victim to carry out his attack. In this situation, it is not possible to distinguish between the attacking party and the victim whose device was used in the implementation of cyber warfare. Distinguishing between civilian and military targets in cyber warfare is a fundamental challenge that must be solved, especially if we know that these attacks have the ability to cause civilian deaths, and the inability to distinguish between targeting military facilities without other objectives that do not achieve a military advantage. (protocol I, p. art 52) A good example of this is that in 2008, tensions between Georgia and Russia escalated to a record level, as cyber attackers from Russia were able to cripple communication services and prevent access to services through websites by preventing access to the server. (Danchev., 2008)

In order to achieve the essence of the principle of distinction, it is the responsibility of military commanders to ensure that the focus is on precisely targetable targets. In the sense of the violation, it is not permissible to resort, in accordance with the law of armed conflict, to a cyber-attack that cannot be controlled or predicted, or those procedures that do not take into account the distinction between military and civilian targets to be targeted by a cyber-attack. (Oona A. Hathaway R. C., ,2012)

The degree of reliability varies from the applicability of the principle of distinction depending on the target to be attacked. The application of the principle seems easy if it targets a control system for military air navigation systems, and consequently leads to the destruction of military aircraft. In this case, this image adequately meets the principle of distinction and conforms to the literal content of the principle of distinction. (Oona A. Hathaway R. C., ,2012, pp. 852-853) However, this picture may not respond to this principle, in whole or in part, if the cyber-attack does not guarantee discrimination,

especially if we know the targets to be attacked are not military par excellence. This is because of the use of dual communication networks between civilian (Ahmad Khalil, Challenges to the principle of distinction in Cyber Warfare: Navigating International Humanitarian Law Compliance, 2024, p. 119) and military purposes at the same time, ninety-five percent of these networks being originally of a civilian nature, (Eric Talbot Jensen, 2010,, p. 1533). As a result, the issue of discrimination sharply raises, especially if the consequences affect civilian and civilian targets significantly and fundamentally. This makes the commitment to maintain the requirements of the principle of discrimination in cyber warfare a difficult challenge to achieve compared to conventional warfare.

Based on the above, both combatants, civilians directly participating in hostilities, and civilians who carry out a combat function continuously, are legitimate targets in cyber warfare in accordance with the Law of Armed Conflict. (Article 51(3) Protocol Additional I.) The contribution of civilians to this type of war makes it difficult to distinguish the legal status of civilians involved in cyber attacks from continuous and direct participation. (International Committee of the Red Cross, 2009)The designer in conflict, who is a civilian, who carries out the function of preparation, control, and implementation, in cyber warfare is seen as a direct participant, which can apply to all civilians who do similar work, and change their legal status from protected categories to legitimate and potential targets of any attack. Although the principle that a civilian who directly participates in hostilities or who adopts a continuous combat function may be lawfully attacked is not in dispute, the status of a civilian who provides indispensable, contemporaneous assistance in cyber-attacks remains unresolved....” (Geoffrey S. Corn, (2008), pp. 286-287).

As the complex situation of technology in cyberspace, calls for the use of civilian experts by the armed forces in order to launch a cyberattack. The practical reality also often proves the army's lack of advanced experts in dealing with cyberspace, which necessitates them to use civilian expertise to carry out cyber-attacks, which makes civilians directly involved in hostilities, and then legitimate military targets in accordance with international humanitarian law. (Ahmed, (December 15, 2018), p. 4)

In that context and highlighting the specificity of the damage caused by an armed conflict within the framework of cyber warfare, the bombing of the electric power production plant for military purposes by a bomb destroys the

plant and the production of electric power is interrupted. The same result will occur, if the attacks are cyber, so that the computer stops running the station due to a failure of the software to carry out its work. (Mateusz Piatkowski, 2017, p. 275) This proves the peculiarity of an impact-based approach to cyberattacks because they are not as kinetic in themselves as is typical in traditional armed conflicts. (Mateusz Piatkowski, 2017, pp. 275-276), (Schmitt, (2008, p. 94)

Thus, it can be said that cyberwarfare's compliance with the principle of distinction is differentiated, so that it is total consistency in narrow and specific cases, and partial consistency in many cases. This is due to the context in which cyber warfare takes place on the one hand, and the specificity of this type of cyber warfare. It is therefore necessary to review and update the relevant legal texts in order to make them consistent, consistent and in full compliance with the principle of distinction, which is the cornerstone of international humanitarian law.

Conclusion:

After addressing the subject of cyber warfare compliance with the principle of distinction in the light of international humanitarian law, we were able to reach the following conclusions and recommendations:

First : Results :

- Cyberwarfare is a new type of warfare that responds primarily to the law of armed conflict, often because it meets the requirements of international armed conflict.
- Cyber wars committed by individuals or entities that are not supported by the state pose a real problem in their legal adaptation because of the failure of the state to adopt these attacks and the difficulty of proving the state's responsibility for these attacks, because the attacking party cannot be identified in most cases, especially in the event that the attacking party evades responsibility for admitting to committing cyber-attacks.
- Cyberwarfare meets the requirements of compliance with the principle of distinction in a differentiated manner, which is total in a few cases, and partial in other cases, especially the issue of direct participation in hostilities that differ from what is usual in traditional warfare. This makes it imperative to reconsider the specificity of the provisions

governing cyberwarfare and the nature that avoids those that characterize classic armed conflicts.

- The means used in cyberwarfare are fundamentally different from those used in classical armed conflicts, as digital space, communications means and the Internet are among the tools and methods used in cyber-attacks.

Second, Recommendations :

- The nature and specificity of cyber warfare and the scope of its implementation in cyberspace make the application of international humanitarian law meet some challenges in defining the concept of cyber warfare and what distinguishes it from it. It also raises more than one concern regarding the applicability of the conditions of international armed conflict due to the different patterns of conventional warfare from this new type of warfare. Accordingly, we suggest updating international humanitarian law and keeping pace with this type of war.
- The nature of the methods and means used in cyber warfare is fundamentally different from those of classical armed conflicts, and therefore a legal framework must be developed that defines the legitimate methods and means that can be subjected to the principle of distinction in order to achieve the goal of protecting civilians and civilian objects.
- Conclude a legal agreement that defines the forms and patterns of cyber warfare to which IHL applies without regard to the consequences it causes, because the implications of cyber warfare are different from those of traditional armed conflicts.
- The principles established by international humanitarian law, in particular the principle of distinction and the need for cyber warfare to comply with it, must be adhered to in a context consistent with the digital environment and the means used in the cyber-attack, and in a manner that does not contradict the content of the principle of distinction.