Oxford International Journal

of Research and Publishing

International Peer-Reviewed Academic Journal

Vol. 1 – No. 1

February - 2025

ISSN (Online): 3050-7618

www.oijrp.com

International Journal of
Research and Publishing

Oxford International Journal of Research and Publishing
International Peer-Reviewed Academic Journal

Volume 1 | Issue 1 | Compilation 1.0

Research 1

Volume 1 | Issue 1 | Compilation 1.0

Oxford International Journal of Research and Publishing https://oijrp.com
2025, Vol. 1, No. 1, 1 - 12

Cyber Warfare in the Light of International Humanitarian Law

Dr. Ahmed Hatem Al-Rubaie
Assistant Professor of International Law - Iraq

Introduction:

In the last ten years, the international community has witnessed a tremendous boom represented by the widespread spread of computer technology and electronic information networks, and this development has radically transformed our lifestyle and the way we interact with the world around us, as access to information has become easier and more flexible than ever before, and reliance on these technologies includes a wide range of essential services and infrastructure that directly affect our daily lives, as their impact has extended to controlling physical systems such as electrical transformers, operating transportation means such as trains, managing health services in hospitals, It has also been used to operate electronic radars and complete commercial transactions, and has expanded to include the management of stock markets and other vital sectors that form the backbone of the modern economy.

Despite the tremendous progress made by the information revolution, at the same time it has created new challenges that threaten the stability of the international community. Cyberspace has emerged as a fifth field of warfare alongside land, sea, air and space. This field has unique characteristics, as it is intangible and unconventional in its movement, which makes it an ideal tool for launching attacks or exercising force without the need to move military pieces or physical assets from one place to another, and the unpredictable nature of this field increases the complexity of dealing with it, as it is difficult to predict when or how it may be used to cause disruption.

The spread of what is known as cyber attacks has contributed to revealing the vulnerability of information networks and the ease of penetration, as a result of over-reliance on the protection programs installed on devices, neglecting to change passwords regularly, neglecting to update systems, and engaging in the use of public Wi-Fi networks or random connections. In addition, major countries seek to exploit cyber attacks as a complementary factor to traditional military attacks, in order to increase pressure and influence on opponents during military operations, and the difficulty of identifying the perpetrator of cyber attacks tempts countries to use these means extensively.

2025, Vol. 1, No. 1, 1 - 12

Problem of study:

The legal issue of the research is centered on trying to answer questions related to the definition of cyber warfare and the applicability of the rules of international humanitarian law to it, as the rules issued by the Geneva Conventions of 1949 and the Additional Protocols of 1977 are still binding on all activities during armed conflicts. However, these rules face challenges due to the evolution of the means and methods of warfare.

The relevance of the study:

The importance of this study is to highlight the potential humanitarian repercussions resulting from the use of cyber operations in cyberspace during armed conflicts, compared to traditional methods of warfare.
When referring to the importance of the topic from the perspective of its novelty, the focus is on cyber warfare, which is regulated by international humanitarian law, as a key axis for defining the framework within which cyber operations can be considered part of the context of an armed conflict or a factor that may lead to it, with the aim of ensuring that such operations are used during armed conflict in line with the relevant international obligations and norms.

Study methodology:

The nature and subject matter of the research requires a heavy reliance on the analytical-deductive approach, with the aim of studying and analyzing the general rules of international humanitarian law to determine the extent to which they can be applied to activities carried out by states and non-state actors in cyberspace, which may be considered or characterized as armed conflict or part of it.

2025, Vol. 1, No. 1, 1 - 12

The structure of the study:

This research deals with the topic of cyber warfare within the framework of the rules of international humanitarian law, as it is divided into two parts, preceded by an introductory introduction, and in the first demand, the concept of cyber warfare will be highlighted through two sections: The first section deals with the definition of cyber warfare, while the second section focuses on analyzing its legal nature. The second requirement will discuss the applicability of the rules of international humanitarian law to cyber operations, and this will be done through two sections, where the first section deals with the comprehensiveness of the rules of international humanitarian law, while the second section studies the specificity of cyber operations and their impact on the applicability of those rules.

At the end of the study, a conclusion will be drawn that presents the most important conclusions and recommendations reached during the study.

First requirement

The concept of cyberwarfare

It will focus on defining the concept of cyber warfare by explaining that the rules of international humanitarian law, as the legal framework governing armed conflicts, do not cover all cyber operations or what is known as cyber attacks based on the comprehensiveness of the term, as the term is used in many areas outside the scope of armed conflict ,These areas include activities related to commercial companies, governments, cybercrime, and other criminal offenses, in parallel with the interest in cyber attacks that fall under the umbrella of international humanitarian law, hence the need to clarify the concept of the term, distinguish it from others that may be similar in meaning, as well as highlight the legal nature of these attacks.

2025, Vol. 1, No. 1, 1 - 12

First Section

Definition of Cyber Warfare

Cyber is a term derived from the ancient Greek word kybermetes, which means remote leadership and management, and has evolved over time to become an umbrella term that reflects the ability to control and direct from long distances, whether in technological, social or even philosophical contexts.(1)

In the terminological concept, Michael N. Schmitt (Michael N. Schmitt) defined cyberattacks as "actions taken by a state to target an adversary's information systems in order to influence and damage them, while at the same time protecting the information systems of the attacking state."(2)

If, depending on the circumstances, cyber attacks result in an escalation of tension to the level of armed conflict, then we are talking about the concept of cyber warfare, which is also known as a cyber attack under the rules of international humanitarian law. This term relates to any cyber operation, whether offensive or defensive in nature, that is likely to result in injury or even death to individuals, as well as negatively affecting property by damaging or destroying it completely, From a broader perspective, cyber-attacks are considered broader in scope than cyberwarfare, as they may fall outside the context of traditional wars, and some of these attacks may even be the first spark that leads to the outbreak of armed conflicts, highlighting their seriousness as a factor that may redefine the concept of international security and the balance of power in the digital world.(3)

Cyber warfare differs from conventional warfare in many aspects, as conventional warfare relies on the use of regular armies and is usually preceded by clear declarations of the state of war, in addition to the existence of specific and direct battlefields, on the other hand, cyber warfare is characterized by its undefined nature in terms of field and objectives, as it relies on attacks launched through global information and communication networks that transcend international borders, and this war relies on a new type of electronic weapons, specifically designed to keep pace with the nature of competition in the information age.(4)

(1) Dr.. Ahmed Abis Naama Al-Fatlawi, Cyber attacks: its concept and international responsibility arising from it in the light of contemporary international organization, Al-Muhaqeeq Al-Halli Journal of Legal and Political Sciences, Babylon University - Faculty of Law, Issue 4, Eighth Year, 2016, p. 614.

(2) 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, Vol. 37, P890.

(3) Philip Levitz, The law of cyber– Attack, 2012, Vol. 100, Issue 4, P833.

(4) Amr Rida Bayoumi, The Dangers of Israeli Weapons of Mass Destruction to Arab National Security, Dar al-Nahda al-Arabiya, 2002, p. 25.

2025, Vol. 1, No. 1, 1 - 12

In 1968, the United Nations Committee on Conventional Arms defined non-conventional weapons as follows: "weapons resulting from nuclear explosions, weapons containing radioactive materials, lethal chemical and biological weapons, and any other weapons that may be developed in the future with destructive properties similar to those of nuclear bombs or the aforementioned weapons."(5)

The reference to "and any other type of weapon manufactured in the future with a destructive effect similar or close to that of non-conventional weapons" is a step towards expanding the traditional concept of these weapons, which includes nuclear, chemical and biological weapons, as this modern concept extends to include damage resulting from cyber attacks in the context of armed conflicts, as cyber attacks may target the computers and information networks of targeted states, exposing civilians to multiple risks, including the loss of basic needs such as drinking water, medical care, electricity, and the disruption of these systems This makes controlling the effects of these attacks extremely complex, which increases the scale of the destruction they can cause if their repercussions cannot be contained.

The definition of the topic raises an important issue related to the characterization of cyber attacks as part of armed conflicts, whether international or non-international conflicts, as this is directly related to international humanitarian law, which is a set of rules aimed at mitigating the effects of armed conflicts for humanitarian reasons, Since the field of application of IHL is limited to armed conflicts, it is first necessary to draw a clear line between situations that can be categorized as armed conflicts and those that cannot. However, this task is difficult when it comes to cyberattacks, especially since these attacks are often carried out in highly irregular circumstances.(6)

Regardless of the issues previously mentioned, cyber attacks are considered part of cyber warfare when they are used in the context of an armed conflict and aimed at achieving military objectives, so they can be defined as actions taken by parties to an armed conflict to gain an advantage over their opponents in cyberspace, through the use of various technological tools and technical experts. These advantages include damaging the enemy's computer systems by destroying them, disrupting them, or breaching them to seize their data. These advantages can also include obtaining sensitive information that the enemy seeks to keep secret, which is known as cyber espionage, or exploiting computer networks to achieve specific objectives within the framework of an armed conflict that rises to the level of war.(7)

(5) Omar bin Abdullah bin Said al-Balushi, "Legality of Weapons of Mass Destruction in accordance with the rules of international law," Manshurat al-Halabi al-Huqqamiya, Beirut, 2007, pp. 15-17.

(6) Omar Mekki, International Humanitarian Law and Terrorism, International Committee of the Red Cross, p. 93.

(7) Herbert Lin, Cyber conflict and international humanitarian law, International review of the red cross, 2012, Vol. 94, N886, P515.

Second Section

The Legal Context of Cyber Warfare

Researching the applicability of IHL rules to cyberwarfare requires first determining the legal characterization of this issue in terms of the legality or illegality of cyberwarfare, in the context of the use of force in international relations, and the relationship between the right to resort to war and the law of war is characterized by a necessary tension, as modern rules of international law generally prohibit the use of force, except in two specific cases: The individual or collective right of states to self-defense,(8) or law enforcement measures adopted by the Security Council.(9)

The law of war aims to strike a balance between the requirements of military operations and humanitarian considerations by imposing clear limitations on the conduct of operations. Despite this balance, the use of force in international relations is illegal under the United Nations Charter, which states that "all Members of the Organization undertake to refrain in their international relations from the threat or use of force in any manner inconsistent with the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes and principles of the United Nations."(10)

This raises the question of the concept of force, whether it is limited to the use of armed force in aggression or armed attack carried out by states through their forces or affiliated groups,(11) or whether it also includes other forms such as economic or political pressure, without limiting it to military force only.(12)

Adopting the first criterion, which relies on the kinetic component of the armed forces, is inconsistent with many forms of use of force in wars, regardless of their legality, such as biological, bacteriological and cyber attacks, while relying on the second criterion expands the concept of the use and threat of force to include economic and political coercion, which may be in line with the objectives of the UN Charter according to the opinion of the majority of scholars, as it expands the concept of aggression and justifies using counterforce based on the right of legitimate defense.(13)

(8) Article 51 of the UN Charter.

(9) Article 42 of the UN Charter.

(10) Article 2 (4) of the Charter of the United Nations.

(11) Alaa al-Din Hussein Makki Khamas, Use of Force in International Law, Military Press Baghdad, 1982, p. 67.

(12) Ibid, p. 68.

In the context of the above, explanatory frameworks for cyber warfare are related to the concept of power, as cyberspace has contributed to strengthening it and controlling its basic elements in international relations, as superiority in this field has become pivotal to carry out effective operations across land, sea, air and space using technological command and control systems, and this calls for redefining power as a system of material and immaterial means and capabilities, visible and invisible, that a state employs to achieve its interests and influence the behavior of other political units.(14)
Another type of cyber warfare is the use of cyberspace as a parallel or supportive arena for a conventional war on the ground. An example of this is what happened in Syria on December 6, 2007, when its air defenses were subjected to a cyber attack targeting a suspected nuclear facility in Deir ez-Zor. The Israeli attack disabled the defenses, allowing the planes to carry out the bombing of the site without detecting the attack. (15)

Second requirement

The applicability of IHL rules to cyber operations

While we have previously touched on the concept of cyber warfare, despite the ambiguity of this concept, in this context we will focus on the use of "cyber attacks" or "cyber operations" in the context of armed conflicts, and these conflicts, whose definition is not disputed, are those in which weapons are used or likely to be used by all or some of the parties.

In this context, we note that the material scope of application of IHL relates to the period of armed conflicts, whether these conflicts are of an international or non-international nature, and this thesis aims to explore the compatibility of IHL rules with cyber operations and their applicability to this type of conflicts.

(14) Joseph Nye, International Disputes - An Introduction to Theory and History, translated by Ahmed Amin El-Gamal and Magdy Kamel, Egyptian Society for the Dissemination of Knowledge and World Culture, Cairo, 1997, p. 82.

(15) Heather Harrison Dinniss, The status and use of computer network attacks in international law, Phd thesis, London school of a economics and Political science, 2008, P 33.

First Section

Principles and Rules of International Humanitarian Law

If we agree that the rules of international humanitarian law do not explicitly refer to cyber operations, the absence of a specific reference does not mean that these operations are excluded from the scope of application of this law, as the general rules of international humanitarian law aim to regulate all methods and means of warfare, including the use of weapons, which makes them comprehensive of technological developments and cyber operations.

This comprehensiveness was emphasized by the article contained in Additional Protocol I to the 1977 Geneva Conventions, which stipulates that "any High Contracting Party, when studying, developing or acquiring a new weapon or instrument of war or a new method of warfare, shall verify its compatibility with the rules contained in this Protocol or any other relevant rule of international law, reflecting the commitment of states to ensure that technological innovations in the field of war do not lead to the violation of humanitarian rules, thus ensuring that international humanitarian law remains a comprehensive and adaptive reference to all forms and methods of armed conflict, including cyber operations."(16)

The core principles of international humanitarian law can be deeply drawn upon when attempting to assess their applicability to the concept of "cyberwarfare" as a form of modern armed conflict. Perhaps the most prominent of these principles is the Martens Clause, the cornerstone of humanitarian protection in the absence of explicit legal rules. This clause, originally established in the preamble of the Hague Conventions of 1899 and 1907, and reaffirmed in Additional Protocol I of 1977 and in the preamble of Protocol II, clearly states that "In the absence of a specific rule of treaty law, belligerents remain under the protection of customary law, the principles of humanity and the dictates of public conscience."

(16) Article 36 of Additional Protocol I to the Geneva Conventions of 1977.

It is worth mentioning the advisory opinion issued by the International Court of Justice on the Legality of the Threat or Use of Nuclear Weapons, in which the Court emphasized the crucial importance of the Martens clause. The Court noted that this clause cannot be questioned as to its continued existence and applicability in various circumstances, regardless of developments in the nature of armed conflicts or the weapons used in them. The Court also emphasized that the Martens clause is an effective and vital means of dealing with rapid advances in military technology, including innovations that may bring about radical changes in the fields and mechanisms of warfare.(17)

We can also cite the judgment of the United States Military Court in the Krupp case in 1948, which highlighted the practical importance of the Martens Clause and went beyond considering it as a mere moral declaration or theoretical principle. The Court affirmed that the Martens Clause constitutes a general legal rule that makes the established customs among civilized nations, the laws of humanity and the dictates of public conscience an integral part of the applicable legal framework, especially in cases where the specific circumstances are not covered by the provisions of treaties.(18)

Consistent with what was mentioned earlier, international humanitarian law scholars agree that there are basic rules that must be observed in armed conflicts, regardless of their nature or level of development. The most prominent of these rules is contained in Additional Protocol I to the Geneva Conventions of 1977. The Protocol emphasizes a very important principle for the protection of civilians, as it explicitly states that: "In case of doubt as to whether a person is a civilian or a non-civilian, that person shall be considered a civilian."(19)

The prohibition of indiscriminate attacks, which aims to protect civilians and civilian objects from harm resulting from indiscriminate hostilities, includes attacks that are not directed at a specific military objective, that rely on means or methods of warfare that cannot be accurately directed at legitimate military objectives, or that use means of warfare whose effects cannot be predicted as required by international humanitarian law, resulting in the injury of civilians and civilian objects in conjunction with military objectives, among other basic principles that are part of the generality of international humanitarian law, as well as the prohibition of indiscriminate attacks, This principle is one of the main pillars of ensuring respect for the rules of distinction in armed conflicts, as it obliges conflicting parties to take the necessary measures to accurately direct their attacks to military targets only, and to avoid causing unjustified damage to civilians. With recent developments in the means of warfare, such as cyber warfare, this principle remains strongly present, as parties must ensure that any cyber attacks do not violate these rules and do not cause indiscriminate damage that unlawfully affects civilians or civilian infrastructure.(20)

(17) Blinding weapons: Reports of the meetings of experts convened by the international committee of the red cross on battlefield laser weapons, 1989– 1991, ICRC, 1993, P 78.

(18) Ibid, P22– 23.

(19) Article 50, paragraph (1) of Additional Protocol I to the Geneva Conventions of 1977.

(20) Article 51, paragraph (4) of Additional Protocol I to the Geneva Conventions of 1977.

Second Section

The specificity of cyber attacks and their impact on the application of IHL principles and rules

Despite the comprehensiveness of the principles and rules of international humanitarian law, the radical changes that have occurred in the nature of warfare since the adoption of the original Geneva Convention more than 150 years ago are undeniable. The means and methods of warfare have evolved to levels not anticipated by the drafters of that convention, and the most prominent manifestation of this evolution is the increasing use of cyberspace for military purposes, which represents a new challenge that highlights the urgent need to review the rules governing the conduct of armed conflicts, and this requires formulating these rules in a way that accommodates the nature of modern cyber uses to ensure their compatibility with legal principles.(21)

In the context of applying the principle of distinction to cyberattacks, the Tallinn Manual, while not mandatory in its rules, notes that civilian objects may not be targeted through cyberattacks, and emphasizes that, for example, cyberattacks that may lead to the destruction of civilian systems or infrastructure are prohibited, This reflects a practical application of the principle of discrimination in the context of cyberspace, as it obliges parties involved in conflicts to take care not to harm civilian infrastructure or non-military objects. This highlights the importance of taking into account the rules of international humanitarian law when using modern technology, ensuring a balance between military necessities and protecting civilians from harm resulting from armed conflicts.(22)

This reality increases the likelihood that attacks will result in widespread collateral damage that may affect vital services such as health, water, energy, or communications. In light of these difficulties, determining whether collateral damage is proportionate to the expected military advantage becomes a practical and legal challenge, requiring the development of tools and criteria for assessing proportionality in this context, to ensure compliance with the principles of international humanitarian law and to protect civilians from unjustified harm.(23)

(21) Jeffrey T. G Kelsey, Hacking in to international humanitarian law: The principles of distinction and neutrality in the age of cyber warfare, Michigan law review, 2008, Vol. 106, Issue7, P 1437.

(22) Michael Schmidt, Warfare through Communication Networks, Attacks on Computer Networks and the Law of War, International Journal of the Red Cross, 2002, p. 105.

(23) Dr. Ahmed Abis Naama al-Fatlawi, op. cit., p. 638.

With regard to the principle of military necessity, the Tallinn Manual indicates that when there are multiple options between military objectives that could achieve a similar military advantage, the objective that is expected to cause the least possible risk to civilians and civilian objects should be selected, requiring the attacker to make the most humane decision and minimize collateral damage as much as possible.
The manual also states that if there are multiple military targets, but one provides a greater military advantage than the others, the attacker is entitled to target that target directly to achieve the greatest possible military advantage in the context of armed conflict. However, consideration must be given to the potential damage to important civilian infrastructure and facilities, as well as the effects on civilians of being deprived of the services or functions provided by those facilities.(24)

The application of the principle of military necessity in cyber attacks requires a balance between achieving military advantage and minimizing harm to civilians, especially since targeting cyber infrastructure may lead to far-reaching repercussions, such as the disruption of vital services such as electricity, telecommunications, or health care, so respecting this principle becomes essential to ensure that cyber military operations remain within the limits imposed by international humanitarian law.

Conclusion:

After a brief review of cyber operations in the context of the major technological transformations that the world has witnessed, through the development of computers as a tool for processing and preserving information digitally and the emergence of the Internet as a means of communication and transmission of information at high speed through data sent over the air, cyber attacks have emerged as a complex phenomenon that can manifest as internal crimes, and these crimes require effective legal treatment through penal and regulatory legislation that criminalizes illegal access to websites and information systems owned by others, with the aim of protecting digital rights and property.
At the international level, there is an increasing need for cooperation between countries to confront these cybercrimes, which often target major financial and banking institutions, as well as companies specialized in programming communications systems and data management. This cooperation requires a comprehensive international legal framework that supports information exchange and coordination between the concerned agencies, to ensure an effective response to these crimes and enhance the security of cyberspace as part of the global system.

(24) Hisham Bashir, Introduction to International Humanitarian Law, 1st edition, National Center for National Publications, Cairo, 2012, p. 89.

After that reference, it became necessary to delve deeper into the study of cyber attacks as part of the threats that affect the military and political levels during armed conflicts, as these attacks have reshaped the concept of means and methods of combat in an unprecedented way, which made them the focus of our research, and through this research, we were able to draw the following conclusions and recommendations:

1. The use or threat of force in international relations is unlawful according to the principles of contemporary international law. However, different interpretations of the term "force" are raised in relation to cyber-attacks, between a standard that links it to the kinetic elements of the armed forces, and another that includes any use of force that results in a violation or tangible impact on the national security of another state.
2. Applying the principle of distinguishing between combatants and non-combatants to military cyberattacks, especially offensive ones, presents a very complex challenge, as the attacker is often thousands of kilometers away from the targeted location, making it difficult to accurately distinguish between military targets and civilian objects, and increasing the risk of indiscriminate or unintentional damage due to the nature of cyberspace and its global interconnectedness.
3. The absence of clear criteria for the use of cyber attacks during armed conflicts complicates the application of the principle of military necessity, especially with the targeting of dual-use facilities that serve both military and civilian efforts, and this overlap raises challenges in the balance between achieving military advantage and protecting civilians, requiring careful regulation to ensure adherence to international humanitarian law.
4. The assertion of the principle of proportionality in the context of cyberattacks appears to remain ambiguous. This principle requires that an attack be canceled or suspended if it is determined that the intended target is non-military or specially protected, or that the attack may result in loss or damage to civilians and civilian objects that outweighs the expected direct military advantage. With the complex nature of cyber attacks, the application of this principle becomes more challenging, requiring precise criteria to assess potential damage and effects.
5. From our findings, despite the difficulties facing the application of IHL principles and rules to cyber attacks, these difficulties should not be compared to an idealized hypothetical case of conventional warfare, but rather the possibility of developing cyber programs to ensure their compatibility with the optimal application of IHL rules, thus enhancing adherence to humanitarian principles even in the context of modern armed conflicts.
6. Broadening the interpretation of IHL principles, such as the Martens Clause, is necessary to cover changing circumstances, especially with regard to modern means and methods of warfare such as cyber-attacks. Such an interpretation ensures the protection of civilians and combatants in accordance with the principles of humanity, while strengthening the law's ability to keep pace with technical innovations and fill emerging legal gaps.
7. Recognizing state responsibility for the actions of individuals or groups under its direction or control, including violations through electronic programs, ensures accountability for international violations, enhances individual criminal responsibility, and allows for the prosecution of those behind the direct perpetrators of such crimes to achieve comprehensive justice.

International Journal of
Research and Publishing

Oxford International Journal of Research and Publishing
International Peer-Reviewed Academic Journal

Volume 1 | Issue 1 | Compilation 1.0

Oxford International Journal of Research and Publishing

2025

www.oijrp.com

ISSN-3050-7618