LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 11(2025)

THE LEGAL REGIME OF CYBER WARFARE

Dr. Boukredine Hiba[1]

[1]Lecturer A, Badji Mokhtar – Annaba University, Algeria
ORCID: https://orcid.org/my-orcid?orcid=0009-0004-7679-9928

hiba.boukredine@univ-annaba.dz[1]
Corresponding author email: boukredinehiba@ymail.com

Received: 16/02/2025 Accepted: 28/08/2025 Published: 03/10/2025

Abstract
Cyber warfare represents a significant evolution in combat methods during armed conflicts. This research is important because it reveals the modern technologies employed in armed conflicts and distinguishes between electronic warfare directed against states in peacetime and cyber warfare in times of armed conflict. This research aims to explore the applicability of the rules and provisions of international humanitarian law, as set out in the 1949 Geneva Conventions and their protocols. In this article, we will discuss the issue of determining the legal framework for cyber armed conflicts in light of the absence of an international treaty governing this type of conflict, especially since it often violates the rights of many protected groups, both public and private.

Keywords: cyber attacks, cyber warfare, international humanitarian law.

Introduction:

Cyber warfare is a significant development in combat methods during armed conflict. This form of warfare has become more important due to the increased use of electronic and informational media, as well as military technologies, in various areas. Consequently, states have moved beyond the traditional realms of land, sea and air warfare to encompass new digital technology-based domains. However, cyber warfare is not explicitly addressed in the four Geneva Conventions or the additional protocols of 1977. Instead, it has been discussed by experts in the 'Tallinn Manual'.

The objectives of studying this topic are as follows:
1) To clarify the specifics of cyber attacks during armed conflicts.
- To distinguish between cyber warfare and electronic warfare.
- To assess the applicability of international humanitarian law to armed conflicts.
We will rely mainly on the following legal foundations: the four Geneva Conventions of 1949; the additional protocols of 1977; and the Tallinn Manual.
Based on the above, we present the following issue: To what extent do conventions related to international humanitarian law contribute to establishing a legal framework for cyber-armed conflicts?
To address this issue, we will employ the following methods:
Content analysis method: to analyse various international agreements that clarify the legal regime for cyber-armed conflicts.
Descriptive method: This method will be used to clarify the forms of cyber-attacks.
The structure of the topic will be as follows:
Chapter One: Defining the concept of cyber armed conflicts.
Chapter Two: The extent to which the rules of humanitarian law can be applied to cyber armed conflicts.
Chapter Three: Examples of cyber armed conflicts.

Chapter One: Defining the Concept of Cyber Armed Conflicts

The 21st century has seen the introduction of numerous domestic, regional and international laws and agreements that directly or indirectly regulate many issues related to information[i]. This includes the emergence of terms such as 'cyberspace', 'cyber attacks', 'digital privacy', and more. However, cyber warfare has not yet been addressed by international or even regional agreements. This has prompted us to define the concept of cyber armed conflict and distinguish it from similar concepts[ii].

Section One: Definition of Cyber Armed Conflict

Cyberspace is considered the fifth domain of warfare, alongside land, sea, air and space. What distinguishes this domain as a means of using force or launching attacks is that it may be used in an unauthorised or illegal manner, causing disruption to the opponent's systems[iii].

First: Jurisprudential definition of cyber armed conflict

Due to the lack of international agreements addressing this type of conflict and due to its novelty, scholars have not reached a consensus on the definition of cyber armed conflict[iv].

Cyber armed conflict is defined as follows: 'The use of multiple electronic activities aimed at weakening, destroying or corrupting computer systems or transmitting information through them using computer networks.' In this context, a cyber attack contributes to the destruction of machines that are computer-controlled.[v]'

Michael Schmidt defined it as follows: 'A set of actions taken by a state to attack enemy information systems with the aim of impacting and harming them while simultaneously defending its own information systems.[vi]'

Efforts to alter, disrupt or destroy computer systems, networks, information or software can damage computer networks, physical facilities or individuals[vii]. Damages resulting from cyber-attacks can range from malicious hacking and website defacement to the widespread destruction of military infrastructure and cities.

Secondly, the definition of cyber armed conflict by international bodies.

Several organisations have defined cyber armed conflict, including:

The United Nations Security Council defined it as the use of computers or digital means by a government, or with the explicit knowledge or consent of a third party acting on behalf of a government, against other states or private property within another state. This includes authorised access, data interception, destruction of digital infrastructure and production and distribution of devices that can be used to disrupt domestic activities[viii].

- The International Committee of the Red Cross: defined it as: 'The actions taken by parties in a conflict to gain an advantage over their opponents in cyberspace using various technical tools and human-dependent techniques. Theoretically, advantages can be achieved by damaging, destroying, impairing or looting the opponent's computer systems (cyber-attack), by obtaining information that the opponent prefers to keep confidential (cyber-espionage), or through cyber-exploitation[ix].
- The Tallinn Manual defined it as: 'All cyber operations, whether offensive or not, that are believed to cause injury or death to humans or damage to physical objects.[x]'

From the above definitions, we can conclude that damage caused by cyber armed conflicts is characterised by:

- widespread damage;
- Long-lasting effects, meaning their impacts persist over time.

Purposefulness, implying that the use of this weapon or means is intended to be widespread and long-lasting[xi].

However, these definitions neglect the fundamental role of the human element in executing these attacks. Furthermore, they converge in focusing on electronic means and targets (computers and related entities)[xii].

Section Two: Principles and Performance of Cyber Armed Conflict

First: Principles of Cyber Armed Conflict

Cyber armed conflict is based on the following principles:

Absence of physical constraints: cyber attacks traverse physical cables.

- Stealth: electronic infiltration.
- Changeability and inconsistency: the methods used to deal with different software and hardware vary due to their differences.
- Identity and privileges: impersonation or causing harm.
- Exceptional use: peaceful use can result in harm to information systems, whereas kinetic actions result in physical damage during a confrontation.
- Infrastructure monitoring: Poor control over infrastructure makes it vulnerable to breaches[xiii].

Second: Tools of Cyber Armed Conflict

Cyber armed conflict relies on the following tools:

Devices: computers and their systems, as well as cables, satellites, routers, etc.

- Software: Cyber warfare depends on malicious software designed to harm the opponent[xiv].

Section Three: Distinguishing Cyber Warfare from Similar Concepts and Its Gradations.

First: Distinction between cyber warfare and similar concepts

1. Cyber warfare vs. cyber attack

As discussed previously, the concept of cyber warfare differs from that of a cyber attack. A cyber attack can occur at any time and may serve as a catalyst for war. However, if it occurs during an armed conflict, it is described as cyber warfare, as it constitutes part of the ongoing conflict[xv].

2. Cyber warfare vs. electronic warfare:

Electronic warfare pertains to military applications within cyberspace and focuses on jamming communication systems, radar and warning devices. In contrast, cyber warfare relies on weapons such as viruses, worms and embedded Trojan time bombs, as well as information warfare. Traditional means such as jamming communication systems are also employed[xvi].

Unlike electronic warfare weapons, the aforementioned tools are used in cyber warfare between states[xvii]. Such warfare must comply with international humanitarian law and adhere to the following principles:

- Principle of distinction: it is prohibited to direct attacks against civilian infrastructure.
- Principle of Proportionality: There must be a balance between the harm inflicted on the opponent and the anticipated military advantage of using force during military operations.
- Principle of humanity[xviii].

Thus, unlike electronic warfare, which reaches the level of war due to the damage it inflicts, we conclude that cyber warfare is a new form of warfare subject to the provisions of international humanitarian law.

Secondly, there are different levels of cyber armed conflict:

- Cold cyber warfare involves the use of various means, including psychological warfare, espionage and the propagation of ideas[xix].
- Medium intensity cyber warfare: This level involves cyber warfare through hacking into websites, storing information and launching attacks.
- Hot cyber warfare: This type of conflict includes remote control over all technological means, potentially leading to 'technological hegemony'[xx].

Chapter Two: The applicability of international humanitarian law to cyber armed conflict

The increasing reliance of states on cyberspace to launch cyber-attacks during armed conflicts has put the principles and rules of international humanitarian law to a complex and real test regarding their applicability to this new type of warfare. The legal regulations relating to the means and methods of warfare were codified at a time when cyber attacks did not exist. The Hague Conventions

of 1899–1907, the four Geneva Conventions of 1949 and the Additional Protocols of 1977 were established without any mention of cyber attacks. This means that there are no special legal provisions governing their use.

In light of the provisions of the law of war, the development of new means and methods of combat was to be expected. Article 36 of the First Additional Protocol to the Geneva Conventions states: 'When studying or developing a new weapon or method of warfare, a High Contracting Party shall determine whether its use would be prohibited in any or all circumstances under this Protocol or any other applicable rule of international law.'

Thus, this article establishes the general framework for regulating the use of new means and methods of combat in armed conflicts. According to the law of war, the provisions of this article indicate that states acquiring modern weapons or developing a new method of warfare must assess their legality. It implies that all rules of the law of war apply to modern means and methods of combat and, in the absence of a specific rule, the general rule applies, at least in principle.

Conversely, Article 36 of the First Additional Protocol does not prohibit developing or acquiring modern weapons or even possessing undefined arms or adopting unregulated new methods under international humanitarian law. Therefore, the provisions of this article do not restrict states' rights in this regard; rather, they stipulate the necessity of legal review when acquiring new types of weapons or developing modern methods, known as legal compliance with international law before their use[xxi]. Thus, this text does not constitute new law but codifies the customary legal principle requiring states to apply treaties or customary rules in good faith, particularly concerning international rules governing combat operations.

The Martens Clause, based on the principles of international humanitarian law, is an effective means of addressing technological developments in the means and methods of combat. First included in the Second Hague Convention of 1899, it states: 'In cases not covered by the law of treaties or customary law, civilians and combatants shall be protected by the principles of international law derived from settled custom, the dictates of public conscience and humanitarian principles.' Consequently, weapons that are abhorrent to public conscience can be prohibited[xxii].

Furthermore, new means and methods of warfare present legal and practical challenges in ensuring that they comply with existing international humanitarian law and take into account the anticipated humanitarian consequences[xxiii]. The right of parties to choose their means and methods of warfare is limited by respect for the principles and laws of armed conflict. International humanitarian law prohibits the use of means and methods of warfare that are indiscriminate, cause excessive damage, or result in unnecessary suffering.

Therefore, this legal framework sets out the constraints and limits on the use of means and methods of warfare. As we enter an era of this new type of warfare, the danger associated with new means and methods of combat lies in the absence of direct confrontation and human judgement. Hostilities must remain within the intended purpose of warfare: to defeat enemy forces and compel their surrender. This ensures that the means and methods employed do not become brutal.

Cyber attacks can target various sectors, including economic, security, agricultural and industrial, within the framework of armed conflict. Several attacks in the past have successfully disrupted the supply of essential services to civilian populations, affecting protected sectors such as health services under international humanitarian law. These cyber-attacks have also affected civilian infrastructure essential for the survival of the civilian population, as well as other infrastructure containing hazardous materials, which are also protected under the law of war.

International humanitarian law establishes a set of rules aimed at mitigating the effects of armed conflicts, whether international or non-international. These rules ensure that fundamental principles govern the choice of means and methods of warfare. The principles of international humanitarian law are based on the idea that they do not prohibit combat actions in armed conflicts, but rather exist to

restrict the means and methods of combat in such conflicts. For this reason, it is acknowledged that all warring parties must accept a certain level of violence, loss of life and destruction as a natural consequence of hostilities. These principles represent the simplest humanitarian foundations applicable at all times and in all places. They provide solutions to unforeseen circumstances and help to address gaps in the law.

Thus, international humanitarian law is based on three principles that govern the conduct of hostilities: distinction, proportionality and humanity.

As outlined in Article 48 of the First Additional Protocol of 1977, the principle of distinction requires parties to an armed conflict to distinguish at all times between civilians and civilian objects, and combatants and military objectives. Additionally, paragraph 2 of Article 51 of the same Protocol states: 'The civilian population as such, as well as individual civilians, shall not be the object of attack, and acts of violence or threats thereof aimed primarily at spreading terror among the civilian population are prohibited.' Furthermore, Article 52 of the same Protocol affirms: 'Civilian objects shall not be the object of attack or reprisals.' Article 55 of the First Protocol also prohibits the use of means and methods of warfare intended to, or expected to, cause widespread and long-term damage to the natural environment and thereby harm the health and survival of the population. Reprisals against the natural environment are prohibited.

Additionally, Article 56 provides protection for engineering works and facilities containing hazardous materials.

The principle of distinction is articulated in many provisions of international humanitarian and customary international law, providing guidance on how attacks should be conducted, alongside the principles of necessity and proportionality.

In this context, the International Court of Justice emphasised in an advisory opinion in 1966 that international humanitarian law is based on two fundamental principles. The first principle states that states must not target civilians, while the second prohibits the use of weapons that would cause unnecessary suffering. This principle is also set out in the 1907 Hague Regulations concerning the Laws and Customs of War on Land, which state that 'the right of belligerents to adopt means of injuring the enemy is not unlimited'[xxiv].

Consequently, given the binding nature of these rules, they apply fully to cyber attacks. In connection with the principle of distinction, only one cyberspace exists that is shared by armed forces and civilian users, and everything is interconnected. The challenge lies in ensuring that such cyber attacks are directed against combatants and military objectives while neutralising civilians or civilian objects that are protected under international humanitarian law. States participating in an armed conflict must exercise caution when employing cyber attacks, bearing in mind that their technical characteristics allow for the precise targeting of specific military objectives only[xxv].

The general rule is that civilian populations may only be attacked if they are directly participating in hostilities, and only for the duration of that participation[xxvi]. Civilians are considered to be directly participating when they engage in specific acts as part of the conduct of hostilities between parties in an armed conflict. Hackers remain protected under international humanitarian law unless they assume a direct role in hostilities. This protection does not exempt them from criminal accountability for any crimes they may have committed. However, if these hackers directly participate in hostilities by conducting cyber attacks in support of one party against another, they lose the protection granted to them against direct attack while carrying out the cyber attack[xxvii].

When applying the principle of distinction to cyber attacks, the Tallinn Manual — despite its non-binding nature — notes that civilian objects must not be targeted in cyber attacks. For instance, cyber attacks that would destroy civilian systems and infrastructure are impermissible unless these systems are considered military objectives that can be targeted in the given circumstances[xxviii].

Based on the above information, it is clear that applying the principle of distinction between combatants and civilians to cyber attacks is extremely complex. Attackers often operate from a considerable distance — sometimes hundreds of kilometres — making it very difficult to ensure compliance with this principle.

It is acknowledged that those controlling this new system of cyber-attacks are far removed from the battlefield. They work under responsible leadership within a military hierarchy that spans everything from planning the attack to issuing and executing orders.

This gives rise to the question: Who bears criminal responsibility for serious violations of the laws of war?

Legal rules only address humans; no matter how advanced the means and methods of combat become, the individual will always be primarily and ultimately responsible for directing and using them. Even as artificial intelligence evolves, there will always be a human at the starting point. Humans are subject to the law, whereas machines or tools are not.

Historically, the state was solely responsible for international crimes committed by individuals acting on its behalf. However, due to the heinous crimes committed by such individuals against humanity and human dignity in the name of the state, individuals have become subjects of international humanitarian law, enjoying rights and bearing obligations[xxix], including individual international criminal responsibility. Scholarly efforts culminated in the establishment of the International Criminal Court at the end of the last century. The Court is tasked with addressing crimes committed by individuals.

Here, responsibility refers to the accountability of leaders and commanders for actions that violate the laws of war, particularly the Geneva Conventions. Scholars have divided this into two types: command responsibility for the acts of subordinates, and individual responsibility as set out in Articles 25 and 28 of the Rome Statute. Criminal responsibility arising from the disruption of civilian communication means during armed conflict is generally governed by the common rules of criminal responsibility set out in international humanitarian law. This law aims to regulate the conduct of combatants and restrict the means and methods of warfare[xxx].

Chapter Three: Models of Cyber Attacks

With the emergence of this new type of warfare, several models have emerged, some of which we will discuss.

Section One: Estonia Model

Estonia is one of the Baltic states that gained independence from the Russian Federation. The country has implemented a series of technology-based reforms across various fields, including the economy, politics and society. It joined the European Union and NATO to enhance its security and free itself from Russian constraints. However, in 2007, it suffered a series of cyber attacks, including 'BOOT NET' attacks and mailbombing. The former aimed to take control of as many computer networks as possible, while the latter sought to inundate users with messages, causing email services and various government services, including banking, to stop functioning.

Russia also employed 'war dialling' technology, initially targeting telephone lines and subsequently focusing on sensitive official websites.

From this analysis, we can conclude the following regarding the Russian strategy:

- Transitioning from direct destruction to pressure and influence.
- Moving from the complete eradication of the enemy to internal dismantling.
- Shifting from traditional battlefields to intimidation and psychological warfare.
- Evolving from surface warfare to extensive cyber warfare.

Progressing from short wars to the use of modern technologies[xxxi].

Section Two: The Russian–Ukrainian Conflict

The Russian-Ukrainian cyber armed conflict began in 2009 as part of a broader information warfare campaign against NATO and the European Union. However, the war officially escalated in 2014 when the Russian president ordered the annexation of Crimea. Russia amassed its army on the Ukrainian border, prompting Ukraine to launch various attacks, including denial-of-service attacks, network intrusions and electronic espionage. Several attacks were launched over a period of days to disrupt the presidential elections[xxxii].

Thus, the Russian-Ukrainian war commenced with cyberattacks that evolved into a ground war. This leads us to conclude that these cyberattacks qualify as the initial phase of a cyber-armed conflict.

Conclusion:

From the above discussions in this research paper, we can conclude the following:

First, results:

Cyber warfare is considered a form of war in the context of international armed conflicts, involving attacks designed to weaken the warring parties.

Various scholars emphasise the need to apply the comprehensive provisions of international humanitarian law to cyber-armed conflicts, despite this type of conflict not being explicitly recognised in the four Geneva Conventions of 1949 and the two additional protocols of 1977. This is due to the connection of such conflicts with the enforcement of humanitarian protection rules, especially since they cause significant damage.

The legal qualification for criminalising aggressive cyber operations holds states accountable for cyberattacks that cause harm to another state.

Warring parties that employ cyber attacks can accurately identify military targets, thus respecting the principle of distinction between military and civilian objectives.

Second/Recommendations:

1. It is essential to recognise cyber-armed conflict as a new type of conflict within the Additional Protocols of 1977.
2. Military leaders who use cyber attacks as a mechanism in conflicts should be held internationally responsible for the damage they cause.
3. International cooperation in cybersecurity is essential to ensure safety in cyberspace.
4. The concept of territorial integrity included in the United Nations Charter should be clarified to encompass critical infrastructure that utilises modern technological means.

References:

Books:

1. Mohammed Saadi, The Impact of Emerging Technology on International Law, Dar Al-Jamia Al-Jadida, 2014.
2. Ahmed Eissa Ni'mah Al-Fatlawi, Cyber Attacks: A Legal and Analytical Study of the Challenges of Contemporary Regulation, Zein Legal, Lebanon, 2018.
3. Adel Abdel Sadiq, Patterns of Cyber Warfare and Their Implications for Global Security, Al-Siyasah Al-Dawlah, Cairo, 2011.
4. Hassan Mufarrah Al-Razoo, Cyberspace, First Edition, Arab Unity Studies Centre, Beirut, 2008.
5. Amir Farag Youssef, Combating Electronic Terrorism: Digital Terrorism in Light of International Agreements, Al-Wafa Library, Alexandria, 2011.
6. Ali Hassan Baker, Electronic Wars in the Twenty-First Century, Center for Crime in the Twenty-First Century, Qatar, 2010.
7. Ashraf Abdel Aziz Al-Zayat, International Responsibility of Heads of State, Dar Al-Nahda Al-Arabiya, Cairo, 1st edition.
8. Ahmed Eissa Ni'mah Al-Fatlawi, Cyber Attacks: A Legal and Analytical Study on the Challenges of Contemporary Regulation, Zein Legal, Lebanon, 1st edition, 2018.

9. Adel Abdel Sadiq, Does Electronic Terrorism Represent a New Form of International Conflict?, Center for Political and Strategic Studies, Cairo, 2017.
10. Nils Melzer, Interpretative Guide on the Notion of Direct Participation in Hostilities under International Humanitarian Law, International Committee of the Red Cross, 2010, p. 20.
[ICRC reference: https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection]

Articles:

1. Ahmed Eissa Ni'mah Al-Fatlawi, 'Cyber Attacks: Their Concept and International Responsibility Arising Therefrom in Light of Contemporary International Regulation', Al-Muhqiq Al-Hilli Journal of Law, Issue 4, 2016.
2. Zainab Shnouf, 'War in the Digital Age: Post-Clausewitz Wars', Algerian Journal of Security and Development, Vol. 9, No. 2, 2020.
3. Adel Abdel Sadiq, 'Patterns of Cyber Warfare and Their Implications for Global Security', International Politics, Cairo, 2011.
4. International Committee of the Red Cross, 'International Humanitarian Law and Cyber Operations during Armed Conflicts', November 2013. Available at:
[ICRC link] (https://www.icrc.org/ar/law-and-policy/cyber-and-information-operations#:~:text).
5. Said Darwish, 'Cyber Wars and Their Impact on Human Rights', Algerian Journal of Legal, Economic and Political Sciences, Issue 54, Volume 5, p. 181.
6. Amani Essam, 'Russia's Use of Cyber Power in Managing Its International Interactions', Journal of the Faculty of Economics and Political Science, Cairo University, Vol. 22, No. 4, October 2022, p. 6.
7. Maizi, L. and Haqati, A., 'Hybrid Warfare in Russian Military Strategy: The Case of the War in Ukraine', Journal of Constitutional Law and Political Institutions, Issue 2, Volume 6, 2022.
8. Jamal Fourar Al-Aidi, 'The Russian-Ukrainian War and Its Implications from the Perspective of International Law', Global Politics Journal, Vol. 7, No. 2, 2023, pp. 150–153.
9. Hurt Lind, 'Cyber Conflict and International Humanitarian Law', International Review of the Red Cross, available at:
ICRC Article: https://international-review.icrc.org/sites/default/files/12825_cyber_conflict_and_international_humanitarian_law.pdf
10. Philip Levitz, 'The Law of Cyber Attack', Vol. 37, Issue 49, 2012.
11. Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', Columbia Journal of Transnational Law, Vol. 37, 1998–99.
12. Michael Robinson, 'Cyber Warfare Issues and Challenges', Computer and Security, Vol. 49, 2015.
13. Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', Int'l Comm. OF THE RED CROSS (19 Nov. 2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.
14. Herbert Lin, 'Cyber Conflict and International Humanitarian Law', International Review of the Red Cross, Vol. 94, 2012.

Conference Proceedings:

1. Louis Dusold-Bec and Anna Newton, Modern Weapons and International Humanitarian Law, Scientific Symposium on International Humanitarian Law: Reality and Aspirations', International Committee of the Red Cross, University of Damascus, Faculty of Law, 2000.
Available at: ICRC link: https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection1-1

Footnotes:

[i]- Philip Levitz, 'The Law of Cyber Attack', Vol. 37, Issue 4 (2012), p. 890.

[ii]- Ahmed Eissa Ni'mah Al-Fatlawi, 'Cyber Attacks: Their Concept and International Responsibility Arising Therefrom in Light of Contemporary International Regulation, Al-Muhqiq Al-Hilli Journal of Law, Issue 4, 2016, p. 614.

Mohammed Saadi, 'The Impact of Emerging Technology on International Law', Dar Al-Jamia Al-Jadida, 2014, p. 25.

Ahmed Eissa Ni'mah Al-Fatlawi, 'Cyber Attacks: A Legal and Analytical Study on the Challenges of Contemporary Regulation, Zein Legal, Lebanon, 1st edition, 2018, p. 16.

Adel Abdel Sadiq, Patterns of Cyber Warfare and Their Implications for Global Security, International Politics, Cairo, 2011, p. 17.

Michael N. Schmitt, 'Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework', Columbia Journal of Transnational Law, Vol. 37, 1998–99, p. 895.

Zainab Shnouf, 'War in the Digital Age: Post-Clausewitz Wars', Algerian Journal of Security and Development, Vol. 9, No. 2, 2020, p. 91.

[iii]- Ahmed Eissa Ni'mah Al-Fatlawi, 'Cyber Attacks: Their Concept and International Responsibility Arising Therefrom in Light of Contemporary International Regulation', p. 516.

[iv]- Zainab Shnouf, 'The aforementioned article', p. 92.

[v]- Adel Abdel Sadiq, 'Patterns of Cyber Warfare and Their Implications for Global Security', International Politics, Cairo, 2011, p. 17.

[vi]- International Committee of the Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflicts, November 2013, available at :https://www.icrc.org/ar/law-and-policy/cyber-and-information-operations#:~:text

[vii]- Darwish, 'Cyber Wars and Their Impact on Human Rights', Algerian Journal of Legal, Economic and Political Sciences, Vol. 5, Issue 54, p. 181.

[viii]- Michael N. Schmitt, op. cit., p. 891.

[ix]- Hassan Mufarrah Al-Razoo, Cyberspace, First Edition, Arab Unity Studies Centre, Beirut, 2008, pp. 213–323.

[x]- Michael Robinson, 'Cyber Warfare Issues and Challenges', Computer and Security, Vol. 49, 2015, pp. 70–80.

[xi]- Micheal robinnson ,IBID,p89 .

[xii]- Zainab Shnouf, 'The aforementioned article', p. 98.

[xiii]- The lead article advocating this view is Knut Dörmann, Applicability of the Additional Protocols to Computer Network Attacks, INT'L COMM. OF THE RED CROSS (Nov. 19,2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

[xiv]- Knut Dörmann, 'Applicability of the Additional Protocols to Computer Network Attacks', Int'l Comm. OF THE RED CROSS (19 Nov. 2004), http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

[xv]- Adel Abdel Sadiq, 'Electronic Terrorism: Power in International Relations: A New Pattern and Different Challenges, 1st edition, Center for Political and Strategic Studies, 2001, pp. 155–229.

[xvi]- Herbert Lin, Cyber conflict and international humanitarian law, International review of the red cross, 2012, Vol. 94, N886, P515.

[xvii]- Adel Abdel-Sadiq, Electronic Terrorism, Power in International Relations, A New Pattern and Different Challenges, previous reference, p. 157.

[xviii]- Amir Farag Youssef, 'Combating Electronic Terrorism: Digital Terrorism in Light of International Agreements, Al-Wafa Library, Alexandria, 2011, p. 55.

[xix]- Adel Abdel Sadiq, 'Does Electronic Terrorism Represent a New Form of International Conflict?', Center for Political and Strategic Studies, Cairo, 2017, p. 6.

[xx]- Ali Hassan Baker, Electronic Wars in the Twenty-First Century, Center for Crime in the Twenty-First Century, Qatar, 2010, p. 34.

[xxi]- Louis Dusold-Bec and Anna Newton, Modern Weapons and International Humanitarian Law, Scientific Symposium on International Humanitarian Law: Reality and Aspirations', International Committee of the Red Cross and the University of Damascus, Faculty of Law, 2000, p. 152.

[xxii]- Louis Dusold-Bec and Anna Newton, 'The same reference', p. 158.

[xxiii]- Ali Hassan Baker, The Same Reference, p. 90.
[xxiv]- Ahmed Eissa Ni'mah Al-Fatlawi, 'Cyber Attacks: Their Concept and International Responsibility Arising Therefrom in Light of Contemporary International Regulation', in the same reference, p. 642.
[xxv]- Darwish Said, 'The aforementioned article', pp. 186–192.
[xxvi]- Nils Melzer, Interpretative Guide on the Notion of Direct Participation in Hostilities under International Humanitarian Law, International Committee of the Red Cross, 2010, p. 20 .
[xxvii]- https://www.icrc.org/ar/document/cyber-warfare-ihl-provides-additional-layer-protection
[xxviii]- Amir Farag Youssef, The Same Reference, p. 90.
[xxix]- Ashraf Abdel Aziz Al-Zayat, International Responsibility of Heads of State, Dar Al-Nahda Al-Arabiya, Cairo, 1st edition, p. 2.
[xxx]- Amani Essam, 'Russia's Use of Cyber Power in Managing Its International Interactions', Journal of the Faculty of Economics and Political Science, Cairo University, Vol. 22, No. 4, October 2022, p. 6.
[xxxi]- Maizi, L. and Haqati, A., 'Hybrid Warfare in Russian Military Strategy: The Case of the War in Ukraine', Journal of Constitutional Law and Political Institutions, Issue 2, Volume 6, 2022.
[xxxii]- Jamal Fourar Al-Aidi, 'The Russian-Ukrainian War and Its Implications from the Perspective of International Law', Global Politics Journal, Vol. 7, No. 2, 2023, pp. 150–153.