

The Issue of Cyber Warfare Under IHL Provisions**Khemissi Bouguetof^{1*}**¹ Echahid Cheikh Larbi Tebessi University, Tebessa (Algeria)khemissi.bouguetof@univ-tebessa.dz

Received: 11 / 05 / 2025

Accepted: 05 / 10 / 2025

Published: 04 / 11 / 2025

Abstract:

The nature of armed conflicts has changed significantly in recent decades; they are no longer restricted to direct engagements or conventional weaponry. Rather, they increasingly include non-traditional approaches, particularly cyberspace. Rapid technological development has made it possible for governments and occasionally armed groups to launch potentially catastrophic attacks using cyberspace instead of traditional weaponry. Since international humanitarian law was created in very different circumstances than the nature of these new dangers, cyber-attacks now rank among the most urgent issues facing the field.

Keywords: cyber-attacks, international humanitarian, malware, cybersecurity, information warfare...

*Khemissi Bouguetof

I. INTRODUCTION

As cyberspace transforms into a battleground similar to traditional war zones, cyber-attacks have emerged as a frequent tactic in contemporary military conflicts. To weaken the adversary's abilities without resorting to conventional military power, these assaults utilize technological methods to infiltrate, disrupt, or eliminate essential information systems, regardless of whether they are military or civilian. These attacks are characterized for their minimal expense, rapid implementation, and extensive impact. They are also hard to accurately track, providing the perpetrator a significant strategic advantage.

The globe has observed real uses of cyber-attacks in wartime, especially in the Russian-Ukrainian conflict that started in 2022, where Russian attacks focused on energy networks, financial institutions, and Ukrainian media to undermine the nation's essential infrastructure.

Despite the advancement of these attacks, international humanitarian law still seeks to maintain its relevance, as they pose considerable legal problematic, especially regarding their compliance with the principles of IHL.

These principles consist of the differentiation between civilian and military objectives, proportionality, and the need for military action. Moreover, the difficulty in pinpointing the offender complicates global accountability, affecting both the demonstration of violations and the assignment of liability to states.

To tackle these issues, countries are enhancing their cybersecurity abilities by creating digital defense systems to safeguard essential infrastructure, preparing military personnel to operate in the cyber realm, and improving global collaboration for information exchange and coordinated action against cyberattacks.

Objective motives for choosing the topic:

The choice of this topic stems from the progression of modern warfare instruments, where cyberattacks have surfaced as a significant approach to modern conflict alongside conventional warfare.

This highlights the necessity of examining cyber warfare to understand the character of armed conflicts in the 21st century. Numerous cyberattacks in times of conflict aim at vital civilian sectors, including hospitals and energy systems, prompting significant concerns regarding compliance with IHL standards.

The challenge of differentiating between hostile and non-military actions in cyberspace, alongside the dual-use characteristics of numerous digital targets (civilian and military), creates intricate legal problematics requiring thorough examination to grasp their compliance with IHL.

Moreover, a major challenge that international law encounters is the difficulty in identifying the responsible party behind a cyberattack, affecting the prospects for international accountability and justified responses.

Personal motives for choosing the topic:

- ✓ The subject combines contemporary technology with international law, prompting me to investigate their relationship in times of armed conflict.
- ✓ Considering the current global events, especially conflicts that employ cyberattacks as a main weapon, I am curious to assess how equipped international law is to confront this emerging threat.
- ✓ The convergence of these disciplines offers a distinctive chance to assess how well legal frameworks respond to emerging technological challenges.

The primary problematic addressed in this research is:

To what extent can the rules and principles of IHL be applied to cyberattacks conducted in the context of armed conflicts?

The study will adopt a descriptive approach to outline cyberattacks and contrast them with related terms. Furthermore, it will use an analytical approach to review current legal documents and evaluate their relevance to cyber-related incidents.

Importance of study:

This research focuses on cyberattacks, a crucial security issue during wartime, and their legal and security implications. It examines their impact on national stability, particularly in armed conflict where infrastructure is vulnerable. The growing reliance on technology in managing essential sectors makes the analysis of strategies to combat cyberattacks an urgent legal and security imperative.

Study objectives:

- ✓ Explanation of the idea of cyberattacks and distinction from conventional types of aggression.
- ✓ Examination of the characteristics and categories of cyber assaults in times of military conflict.
- ✓ Analysis of global legal structures regulating cyberspace use during conflicts.
- ✓ Emphasizing the difficulties encountered by countries in combating cyberattacks, especially during times of conflict.
- ✓ Providing suggestions to improve cybersecurity and create efficient digital defense tactics in times of war.

To tackle this problematic, the theoretical and organizational underpinnings of cyberattacks will be analyzed through the lens of international humanitarian law in the theoretical portion, whereas the following section will address the legal and practical difficulties of enforcing these regulations in the cyber domain.

1. The Concept of Cyber Warfare

Given the swift technological progress and the intertwining of the digital realm with our everyday existence, cyberattacks have become a growing menace to individuals, organizations, and countries. Consequently, it is crucial to outline these attacks, as they have specific traits that will be examined in this discourse.

1.1 Definition of Cyber Warfare

1.1.1 Linguistic & idiomatic definition:

A- Linguistic definition:

In the linguistics area, cyber (cybernetics) refers to a concept that originates from the Greek term “kybernetes”, meaning leadership and remote management (Cherif, 2021, p.3071; Saoud, 2019, p.83).

It is noteworthy that language dictionaries haven't determined the source of the term “cyber”, aside from references in the Al-Mawrid dictionary, which describes it as “cyber, the science of regulation, derived from the term (cybernetics), which corresponds to the idea of cybernetics, involving the control and oversight of systems remotely” (El-Fatalaoui, 2016, p.614).

According to various military terminology dictionaries, the term “cyber” does not originate from its initial source but is defined in relation to military contexts. The dictionary of American military terms defines it as “any activities carried out via e-networks intended to manage or interfere with other electronic systems” (USDD, 2016).

The Information Security Terminology Dictionary defines the term “cyberattack” as an offensive operation carried out in cyberspace with the goal of gaining control over websites or electronically safeguarded infrastructures to interrupt, destroy, or harm them.

In Arabic, finding a term that closely matches the English word “cyber” is a challenge. The Arabic rendering of the title of the Council of Europe Convention on Cybercrime was incorrect, as the phrase “Convention on Cybercrime” was translated into Arabic as “Convention on E-Crime”. This difference stems from the lack of an equivalent term in Arabic (El-Fatalaoui, op.cit., p.615).

B- Idiomatic definition:

The concept of a cyberattack has been interpreted in numerous ways from various viewpoints, yet these interpretations have a shared core. It pertains to the approach of targeting websites via different communication channels. Included in these definitions is the viewpoint presented by specialists in IHL, particularly Shin, who asserts that “using electronic or electromagnetic spectrum to store, alter, and share information targets systems managing the related infrastructure” (Chamel & Lokman, 2024, p.158).

Fiorets describes it as an online attack that entails breaching legitimate websites to interfere with or eliminate the data they hold or to take control of that information. This represents a succession of cyberattacks executed by one country against another (Amir, 2021, p.9).

Within the sphere of cybersecurity, Michael N. Schmith characterizes cyber warfare as the measures taken by a nation to attack an opponent's information systems with the aim of harming and disrupting them, while simultaneously safeguarding its own information systems against comparable threats (Saoud, 2019, p.84; Himia, 2024).

Citing the Tallinn Manual (N. Schmitt, 2017), he relied on Article 36 of the Additional Protocol I to the Geneva Conventions, established in 1977, which claims there is an international duty to evaluate the legality of all new weapon types.

Supporters who argue for the inclusion of cyberattacks within the scope of IHL reference this provision when such attacks take place during armed conflicts (Tai & Kazem, 2025, p.30; Helsoun, 2025, p.470).

As stated by Cordula Droege, the legal advisor for the International Committee of the Red Cross, cyberattacks are fundamentally actions carried out against or via a computer through the movement of data. These actions may seek to fulfill different goals, such as infiltrating a particular system to gather, move, destroy, change, or encrypt information, or to adjust the operations managed by the hacked computer or manipulate them. In specific situations, these actions may be categorized as attacks based on the definitions outlined in humanitarian law (Rabie, 2024, p.24).

In the framework of employing the principle of distinction in cyber warfare, the Tallinn Manual observes that, while its guidelines are not compulsory, civilian targets should not be attacked in cyber operations, especially those that could dismantle civilian systems and infrastructure, unless they are classified as military objectives that can be justifiably targeted (Derradji & Akkour, 2024, p.4).

Some interpret it narrowly as adjusting computer system functions to hinder adversaries from using them successfully, as well as penetrating information systems and communication networks to gather, hold, and examine the data they contain.

In a wider context, it is characterized as an electronic maneuver, either defensive or offensive, that is reasonably anticipated to result in harm or fatality to a person, or to cause material damage or destruction to the intended target (Cherif, op.cit., pp.3069-3070).

The Tallinn Manual highlights the significance of following the principle of proportionality within the relevant legal framework of cyber warfare, especially in banning cyberattacks that might lead to civilian deaths, injuries, or harm to civilian properties (N.Schmitt, op.cit.).

1.1.2 Aspects on cyber warfare:

A– Characteristics:

Cyber warfare has a number of characteristics, including:

- Cyberattacks are complex technical attacks that embody the height of progress in information technology, software, computing, and communications.
- In contrast to conventional weapons like submarines, aircraft carriers, and modern fighter jets, which necessitate considerable budget commitments from countries, cyber weapons can be created with much lesser financial input.
- Cyberattacks are defined by their quick and covert nature, able to take place at any time, whether in peace or during war.
- In cyber warfare, aggressors possess a unique edge over defenders, unlike in traditional warfare where defenders frequently have strategically advantageous locations. The rapid pace and unpredictability of cyberattacks provide attackers a tactical advantage, enabling them to select when and where to launch their attacks without allowing defenders to foresee the strike, rendering it almost unfeasible to sufficiently secure all cyber targets (Hedib, 2024, p.118).
- It is difficult to determine the whereabouts and identity of those responsible for cyberattacks, as such attacks generally do not leave any signs or proof. The majority are found accidentally and necessitate considerable time and advanced technical expertise to track down their origin (Amir, op.cit., p.11).
- Cyberattacks transcend geographical boundaries, making them easy to launch against any adversary regardless of their location relative to the attacking nation. The consequences of cyber

warfare are extensive, potentially inflicting damage on both military and civilian targets, as well as critical infrastructure within the state (Khedidja, 2024, p.286).

– Cyber warfare is characterized by destruction that does not necessarily involve bloodshed or physical remains. The proliferation of cyberspace and its accessibility has led to an increase in the number of attackers and a broader range of targeted sites. These attacks are also marked by a cat-and-mouse dynamic, reflecting a prolonged state of conflict inherent to the diverse nature of cyberspace (Karrar, 2023, p.23).

B- Differentiating cyber warfare from other forms:

Cyber warfare is different from conventional or traditional warfare and also varies from cyber terrorism. Conventional warfare is classified into conflicts that use standard weapons and equipment like tanks, aircraft, and missiles, or it can include the deployment of weapons of mass destruction.

*** Differentiating cyber warfare from traditional warfare:**

Some have defined traditional warfare as an armed conflict between two opposing parties, where each side utilizes all available weapons and means to destroy the adversary and impose its will, defending its interests and rights (Lmajdoub, 2004, p.623).

The traditional war is defined as “an armed conflict between two or more states aimed at imposing a political viewpoint through means regulated by international law” (Bouadi, 2005, p.10).

- The parties involved must be states or governments, rather than specific groups or individual citizens (Hammouda, 2008, p.42).
- The use of armed force is essential, distinguishing war from other actions such as retaliatory or coercive measures (Atlem, 2002, p.8).
- There must be a mutual intention among the conflicting parties to engage in war, while adhering to the principles of IHL (Cherif, op.cit., p.3078).

Cyber warfare is distinct from traditional warfare in that the latter relies on the deployment of regular armies, preceded by a formal declaration of war and a clearly defined battlefield determined by the conflicting parties.

In contrast, cyber warfare occurs in an undefined arena, where attacks take place in a virtual space, often lacking clear objectives. This form of warfare utilizes advanced electronic weaponry that aligns with the nature of the digital race in the information age, targeting critical infrastructure (Beyoumi, 2002, p.25).

*** Differentiating cyber warfare from cyberattacks:**

Cyber warfare refers to a category of cyberattacks that occur during an armed conflict or produce physical effects comparable to those of traditional military strikes.

In contrast, cyberattacks encompass any harmful activities directed at other nations, whether during peacetime or wartime, that result in significant physical damage to lives or property, or disrupt computer systems, provided these actions are intended for military and security purposes (Chadli, 2025, p.1235).

It is important to note that there are significant differences between cybercrime and cyberattacks (cyber warfare or cyber force). The primary aim of a cyberattack is to undermine the functionality of targeted computer networks in another country to achieve a political objective.

In contrast, cybercrime is perpetrated by an entity that does not represent a state or its institutions, whether it be an individual or a corporate entity. The intent behind cybercrime is criminal, achieved by breaching specific electronic devices for personal gain.

Such actions are only classified as cybercrime if they constitute an offense under domestic criminal law, based on the principle that “Nullum crimen sine lege”, which is one of the fundamental principles underpinning criminal justice systems (Amani, 2024, p.25).

It is important to note that the damages resulting from cyberattacks and cybercrime vary significantly. Cyberattacks are designed to cause widespread harm to both individuals and property in another state, which contrasts with cybercrime, where the impact is generally limited to specific users (Amira, 2020, p.395).

1.2 Forms & consequences of cyber warfare:

This sub-section will explore the various types of cyber warfare and their forms.

1.2.1 Types & forms of cyber warfare:

A- Types of cyber warfare:

*** Cold Cyber War:**

Cyber warfare represents a state of ongoing, unannounced informational conflict between nations within the cyberspace, characterized by efforts to dominate digital and informational infrastructures, all while avoiding direct military confrontations.

According to researcher Thomas Rid, the “*cold cyber war*” represents a prolonged, covert struggle characterized by infiltration, disinformation, and unattributed attacks (Rid, 2013).

It is important to note that the specific activities underpinning the cold cyber warfare include commercial espionage, threats to business interests, breaches of official websites, and the dissemination of anti-state messages by the entities that have been attacked (Hedib, 2024, p.120).

*** Medium-intensity Cyber Warfare:**

Medium-level cyber warfare represents a type of cyberattack that falls between simple, uncoordinated attacks and comprehensive cyber warfare. It is characterized by targeting digital banking systems, energy infrastructures, and communication networks, while also impacting the flow of daily life without causing direct physical destruction or employing conventional military means (Hebib, Ibid., p.121).

One of the most notable examples of the use of such conflicts is the NATO airstrikes on Yugoslavia in 1999, which disrupted the communication networks of adversaries and incapacitated government, banking, and media sites. This pattern continued during the war between Lebanon and Israel in 2016, as well as the conflict between Russia and Georgia in 2008, and the confrontations between Hamas and Israel in 2008 and 2010.

These attacks were employed in Ukraine between 2015 and 2016, targeting the electrical infrastructure and resulting in widespread power outages (Gachti, 2024, p.492).

*** High-intensity cyber warfare:**

Cyber warfare, characterized by its intensity, is defined as an advanced form of digital conflict where organized and intensive cyberattacks are launched against a nation's critical infrastructure. This type of warfare often accompanies or replaces traditional military operations, establishing itself as a distinct battleground. Unlike limited espionage or sabotage, cyber warfare targets control systems for energy, transportation, communications, and healthcare services, aiming to incapacitate the adversary's ability to function as an organized entity (Leclerc, 2017, p.78).

High-Intensity Cyberwarfare represents one of the most perilous forms of contemporary digital conflict, as it targets the critical infrastructure of nations through sophisticated electronic means.

The primary aim is to disrupt state institutions, particularly those related to cultural assets such as museums, heritage archives, and digital preservation platforms that increasingly rely on internet-connected systems. This reliance renders them vulnerable to destruction or breach during such attacks, even if they are not the direct targets, all without the use of conventional weapons (Gachti, op.cit., p.492).

The infamous cyberattack known as NotPetya, which originated in Ukraine in 2017 and spread to critical global institutions, serves as a vivid example of the impact of such cyber warfare. Journalist Andy Greenberg documented its details in his book *Sandworm*, highlighting how a single digital virus was able to inflict losses estimated in the billions of dollars and disrupt essential networks entirely (Andy, 2019, pp.142–178).

One of the most significant transformations in the nature of modern conflicts is represented by powerful cyber warfare, which can incapacitate various systems of targeted nations without the need for direct military force (Hedib, op.cit., p.120).

A key characteristic of this type of warfare is the comprehensive nature of the attacks, as evidenced by the Russian–Ukrainian conflict, which has caused widespread *functional paralysis* (Rid, 2020) within state structures and has been observed in several suspicious cases over the past decade (Singer & Friedman, 2014).

Legally, this form of conflict poses a substantial challenge to international humanitarian law, particularly concerning the principles of distinction between civilians and combatants, as well as proportionality. The 'Tallinn Manual 2.0' has attempted to provide an analytical framework for applying international law rules to these situations, yet it remains merely a non-binding guideline (Schmitt, 2021).

B- Forms of cyber warfare:

These “forms” rely on a variety of techniques, including digital bombs, malware or viruses, denial of service attacks, and worms, highlighting the evolving and alarming nature of these conflicts in our digital world.

*** Digital bombs:**

Digital bombs are cyber offensive tools designed to disrupt or destroy computer and digital systems within the targeted state's infrastructure. Their impact is akin to that of traditional bombs; however, instead of causing physical explosions, they lead to data destruction or the disabling of E-Systems that both civilian and military institutions rely on.

It is important to note that digital bombs are used in cyber warfare, targeting critical systems such as electricity, communications, transportation, and even defense mechanisms, thereby crippling a nation's ability to respond to military attacks.

From a legal perspective, these types of attacks encounter significant challenges, particularly in terms of establishing accountability, as cyberattacks can be difficult to trace back to their source, complicating the enforcement of international liability principles.

Digital bombs are considered offensive tools in modern conflicts, raising significant legal questions, particularly regarding the applicability of international humanitarian law. This includes concerns about the principle of distinction between civilian and military targets, as well as proportionality.

For instance, if a digital bomb is deployed to destroy a civilian control system that is shared with a military facility, it could result in disproportionate damage to civilian infrastructure, which contradicts the fundamental principles of IHL (Ali, 2020, p.45).

One of the primary challenges in addressing digital bombs is the issue of attribution. The attacks carried out using these digital bombs can be shrouded in layers of concealment, making it difficult to definitively identify the perpetrator. This identification is crucial for holding a state accountable under international law (Soror, 2019, p.122).

*** Malware:**

Malware is defined as any software designed to harm computer systems, steal data, or spy on users without their knowledge (Mohammed, 2020, p.45). There are various types of malware, including viruses that spread from one file to another causing system malfunctions, worms that rapidly propagate through networks without human intervention, and Trojans that disguise themselves as legitimate programs to exploit security vulnerabilities (Sami, 2019, pp.88–91).

One of the most dangerous modern types of malware is ransomware, which encrypts user files and demands a financial payment for decryption. This has led to significant losses for economies worldwide. Additionally, spyware and keyloggers are utilized to steal sensitive data and passwords (NCA, 2022, pp11–15).

*** Worm software:**

Worms are a type of malicious software (malware) that fall under the category of viruses, but they are distinct in their ability to replicate and spread independently without needing to attach themselves to an existing executable file or program (Nour, 2021, p.18).

The worm is designed and programmed to exploit security vulnerabilities in operating systems or networks, allowing it to replicate itself across local networks or the internet, which enables it to infect a large number of devices in a very short period (Soror, 2019, p.112).

Worms frequently carry additional malicious software such as Remote Access Tools or spyware, which can result in significant damage including system disruptions, network slowdowns, or excessive consumption of device resources (Sameer, 2021, p.87).

The danger posed by worms lies in their ability to execute programmed instructions autonomously, allowing them to transmit sensitive data to hackers or establish “backdoors” that enable these intruders to gain control over the infected systems at a later time (Hassan, 2021, p.29).

Among the most well-known examples of electronic worms are the Blaster Worm and the Conficker Worm, both of which have caused significant damage to various countries (Eric, 2005, p.132).

*** Trojan programs:**

The Trojan Horse is a type of malware that derives its name from the famous Greek myth in which the Greeks infiltrated the city of Troy using a deceptive wooden horse. This form of software tricks users by presenting itself as a legitimate or beneficial program, while secretly carrying out harmful activities on the user's device or data (Karrar, 2021, p.204).

2. The applicability the IHL rules to cyber warfare and its consequences

There is a divergence of opinions among legal scholars regarding the applicability of international humanitarian law to cyber warfare. Some argue that international humanitarian law cannot be applied to conflicts that differ from traditional warfare, which necessitates a distinct legal framework for regulation. Conversely, others believe that international humanitarian law can indeed be applied to such conflicts through analogy and comparative jurisprudence.

1. The applicability the IHL rules to cyber warfare

There is a scholarly debate regarding the extent to which cyber warfare aligns with the principles of international humanitarian law.

1.1 The non-applicability the IHL rules to cyber warfare

The digital space is characterized by the absence of international oversight capable of exerting control over it. Consequently, a legal perspective has emerged that rejects the notion of regulating the internet, asserting that it is a lawless domain.

This viewpoint is championed by certain American politicians, information technology experts, and some international law scholars, who argue that the internet exists as an independent realm, distinct from all other spaces, including our tangible physical environment. Therefore, they contend that it cannot be subjected to IHL, for (Omar, 2019, p.137):

- ✓ The lack of oversight prevents specialized authorities from controlling internet networks.
- ✓ There is no legal text within international humanitarian law that addresses cyberattacks, as it pertains only to armed conflicts.
- ✓ The initiation of cyberattacks began after the establishment of international treaties related to international humanitarian law, thus placing them outside the scope of its provisions since they are not armed attacks.
- ✓ Legal rules within international humanitarian law govern means and methods of warfare that result in physical effects, which are not applicable to cyberattacks.
- ✓ Traditional warfare is characterized by a clear declaration of war and defined battlefields, relying on regular armies, whereas cyberattacks lack specific domains or targets, as they are executed through cross-border information or communication networks, utilizing new electronic weapons that align with technological advancements, aimed at critical infrastructure (Adel, 2009, pp.155–229).
- ✓ The legal classification of computer attacks is closer to terrorism than to war.
- ✓ The inability to deal with cyberattacks raises a major problem in identifying and understanding cyber weapons.
- ✓ Proponents of this view add that the means and methods of cyber warfare are not sufficiently clear and understood, and that they are carried out in complete secrecy. Therefore, applying the general principles of international humanitarian law to cyberspace is unrealistic.
- ✓ Cyberattacks are also characterized by being preemptive and without prior warning, and their scope and scope are not specific. Their objectives are unknown, and they are not specific to a country, whether it is the target of the war or a participant in it. They are multifaceted and intertwined with media, political, psychological, technological, and terrorist warfare, unlike conventional warfare, whose objectives and location are specific.
- ✓ Cyber fighters do not have a fixed location and do not need to be present in the location where the attack occurs, or even in the location where the attack appears to originate (Omar, op.cit., p.137).
- ✓ Attackers typically conceal their identity using anonymous communication technology and encryption.
- ✓ The difficulty lies in identifying the source of these attacks, which are usually carried out anonymously or through automated robotic software. It is also difficult to trace their perpetrators to assign responsibility to a state, organization, or individual, and to establish a link between these operations. Armed conflict greatly complicates determining whether international humanitarian law applies to this situation. Furthermore, the interconnectedness of civilian and military computer systems further complicates the application of the rules of IHL (Omar, Ibid., p.137).

1.2 The applicability the IHL rules to cyber warfare

Proponents of this view argue that cyberspace is not devoid of legal regulations (Cyberspace is not a “Law-free” zone), asserting that the existing legal frameworks are sufficient to govern the digital realm. They believe these laws can be effectively applied to modern technologies, a perspective known as the legalist doctrine.

Historically, communication methods such as telephones, mail, and fax have been regulated in France, and similar principles can be extended to the internet. Therefore, it is essential for the law to adapt and collaborate with technological advancements, recognizing that many existing legal provisions are applicable to online interactions (Hamed, 2022, p.375).

Proponents of this view assert that IHL applies its rules and principles universally to all forms of armed conflict, both international and non-international, including cyber warfare. While the treaties of international humanitarian law do not explicitly mention cyberattacks, the argument holds significance only under the “*Martinez*” condition, which is a well-established principle in international humanitarian law.

This principle states that in situations not covered by international agreements, both civilians and combatants remain under the protection and authority of humanitarian law principles derived from established customary traditions and humanitarian principles (Souhil, 2012, p.45).

It is important to note that proponents of this viewpoint respond to the opposing argument against applying the law of war to cyber warfare by asserting that the United Nations Charter explicitly requires the use of force for a conflict to be classified as an armed conflict under international humanitarian law. They argue that cyberattacks do not constitute armed conflict as they do not involve the use of force.

However, supporters of this perspective counter that while Article 2, paragraph 4 of the UN Charter prohibits states from threatening or using force against the territorial integrity or political independence of any state, it also leaves the interpretation of this provision to the Security Council, which must consider the evolving circumstances (Hamed, op.cit., p.140).

Upon examining Article 39 of the United Nations Charter, it becomes evident that the Security Council is empowered to assess the situations presented to it and to determine the necessary coercive measures in response to threats to international peace and security, or breaches thereof, including acts of aggression.

Consequently, the Security Council has the authority to classify cyberattacks as threats to international peace and security or as violations thereof, without needing to delve into the specifics of the preceding article (Lamoudi, 2024, p.203).

In this context, Article 36 of the Additional Protocol I attached to the 1949 Geneva Conventions concerning the protection of victims of international armed conflicts states that “any High Contracting Party must ensure that when considering, developing, or acquiring a new weapon or means of warfare, or adopting a method of warfare, it must verify whether it is prohibited in all circumstances or in some cases”.

According to this protocol or any other rule of international law to which the contracting parties are bound, this provision applies to cyberattacks as a weapon or method of warfare.

Therefore, states must ensure the legality of their use in accordance with the rules of this agreement or any other rules of international humanitarian law, which necessitates the application of international human rights law to cyber warfare.

According to international humanitarian law principles, cyberattacks on a state, particularly those that cause significant harm to civilians or damage to the targeted state's infrastructure, are applicable regardless of their intensity.

Legal scholars have reached a consensus that electronic attacks can be classified as legitimate warfare when they have a tangible impact on the physical world, provided that this impact is destructive, thereby invoking the provisions of IHL (Djilali, 2023, P.174) .

Based on the aforementioned points, it is evident that proponents of this perspective unanimously agree on subjecting cyberattacks to international humanitarian law.

This is grounded in the fact that the United Nations Charter has delegated the interpretation of Article 2, paragraph 4, to the Security Council, which assesses the circumstances presented to it. If the Council determines that these circumstances violate international law, they are classified as armed conflicts that fall under the purview of international law, irrespective of the type of weapon used, as long as such actions result in harm to individuals and the infrastructure of states.

Therefore, cyberattacks can be governed by international humanitarian law due to the damage they inflict on individuals and state infrastructure, particularly when such impacts are devastating (Lamouri, op.cit., p.203).

According to proponents of this perspective, they have highlighted the principles governing the use of cyberattacks during hostile operations. It is well-known that parties involved in any armed conflict rely on the use of force, particularly cyberattacks, to either neutralize or at least significantly weaken the military capabilities of their adversaries.

However, international humanitarian law is designed to regulate the use of force rather than prohibit it, and it establishes two fundamental principles that must be respected by all parties involved in the conflict which are:

A– Cyberattacks and the principle of military necessity:

The principle of military necessity aims to incapacitate the enemy by destroying their military, material, and human capabilities, which compels the warring parties to employ specific types of combat means to achieve this objective.

The principle of military necessity aims to select attacks that inflict minimal damage and casualties on civilian objects and individuals. When there are military targets, if one offers a greater military advantage than others, direct cyberattacks may be directed at that military objective to achieve the goals of the armed conflict.

Therefore, it is essential to consider the extent of harm caused to civilians, their facilities, and critical infrastructure, as well as the deprivation of functions and services these facilities provide due to cyberattacks (Cherif, op.cit., pp.3091–3092).

B– Reconciling harm and military benefits:

This principle indicates that military advantage must be gained through specific operations that outweigh the harm inflicted on civilians and civilian objects as a result of such actions. This is reflected in the provisions of Article 57, paragraph 2, clause 3, and paragraph 3, as well as Article 25 of the First Protocol of 1977.

In addition to its prominent treaty-based nature, this principle also exhibits customary characteristics, affirming its status as a fundamental rule within international law governing armed conflicts. Consequently, it applies to all types of weapons utilized in these conflicts, and electronic attacks must adhere to the principle of proportionality (Amir, 2021, p.51).

The principle of balance refers to the reconciliation between military necessity and humanitarian principles, aiming to minimize the human losses resulting from military operations (Lamouri, op.cit., p.204).

2. The implications of cyberattacks from both a military perspective and their impact on civilians

2.1 The implications from both a military perspective

A– Diminishing military capabilities

Cyberattacks disrupt command, control, and communication systems within military forces, resulting in paralysis of combat operations and a loss of effective field coordination (Sami, 2018, p.105).

B– Disruption of defense systems

Cyberattacks are employed to target defense systems such as radars and smart missiles, which can compromise their accuracy or completely disable them, posing a strategic threat to national security (Khaled, 2021, p.47).

C– Intelligence data hack

Cyberattacks enable infiltration into sensitive military information systems and the theft of operational plans or espionage information, affecting the balance of power between opposing parties (Saad, 2021, p.91).

D– The impact on logistical readiness

The attacks are aimed at military supply, logistics, and storage systems, which disrupt the vital supply chain during military operations (Saad, Ibid., p.91).

2.2 The implications on civilians

*** Targeting critical infrastructure**

Attacks result in a paralysis of essential services such as electricity, water, and transportation, directly impacting civilian life, as evidenced by the power outages affecting thousands of homes in Ukraine in 2015 (Ahmed, 2019, p.66).

*** Disruption of healthcare services**

Targeting hospitals and health information systems with ransomware or viruses endangers patients' lives, as demonstrated during the “WannaCry” attack that impacted the healthcare system in the United Kingdom (Mourad, 2021, p.101).

*** Psychological and societal impacts**

Cyberattacks have a significant impact on the mental well-being of citizens, instilling feelings of panic and fear, particularly when they are accompanied by disinformation campaigns or leaks of sensitive information (ITU, 2022, p.45).

II. Conclusion:

Cyber warfare, during armed conflicts, represents a significant evolution in the nature of security threats, as it is no longer confined to traditional battlefields but has expanded into the digital realm, which has become a strategic dimension equally as important as land, sea, and air.

Recent conflicts have demonstrated that cyberattacks are employed as an effective weapon to disrupt critical infrastructure and limit an adversary's capabilities without resorting to direct military force.

However, the international legal framework, particularly in humanitarian law, still exhibits significant shortcomings in regulating this type of warfare, especially regarding the determination

of liability, proportionality, and the distinction between military and civilian targets affected by these attacks. Additionally, the challenges in identifying actors in cyberspace hinder legal accountability efforts and weaken deterrence measures.

Results:

- ✓ Cyber warfare, in the context of armed conflicts, signifies a notable advancement in the landscape of security threats, as it transcends traditional battlefields and has permeated the digital domain, which has emerged as a strategic area of equal importance to land, sea, and air.
- ✓ Recent conflicts have illustrated that cyberattacks serve as a potent tool to disrupt essential infrastructure and curtail an adversary's capabilities without the need for direct military engagement.
- ✓ Nevertheless, the international legal framework, especially within humanitarian law, reveals considerable deficiencies in governing this form of warfare, particularly concerning the assessment of liability, proportionality, and the differentiation between military and civilian targets impacted by these assaults.
- ✓ Furthermore, the difficulties in identifying actors within cyberspace impede efforts for legal accountability and undermine deterrence strategies. • As a result, there is an urgent need for the development of comprehensive legal standards to address the complexities of cyber warfare and ensure effective regulation.

Recommendations:

- ✓ It is crucial to establish clear international treaties that encompass cyberattacks within the framework of armed conflict laws, along with accurate definitions of terms associated with cyber warfare.
- ✓ Countries ought to strengthen their digital defenses by allocating resources to cybersecurity infrastructure and creating dedicated cybersecurity teams. It is important to set forth explicit international standards to safeguard civilian infrastructures, especially hospitals, banks, and power grids from cyber assaults during times of conflict.
- ✓ The development of explicit international agreements that incorporate cyberattacks into the laws governing armed conflict is vital, along with the formulation of precise definitions for concepts pertaining to cyber warfare.
- ✓ Nations must bolster their digital security by investing in cybersecurity infrastructure and assembling specialized teams focused on cybersecurity. It is essential to establish clear international guidelines to protect civilian facilities, particularly hospitals, banks, and power grids from cyber threats amid conflicts.
- ✓ Establishing clear international agreements that recognize cyberattacks within the laws of armed conflict is imperative, along with the need for precise definitions of cyber warfare-related concepts. Countries should enhance their digital defenses through investments in cybersecurity infrastructure and the formation of specialized teams, while also creating international standards to protect civilian entities like hospitals, banks, and power grids from digital assaults during conflicts.

References:**Books:**

1. Abdalla Mohammed Ali (2020), *Cybercrimes and Cyber Threats*, Dar Al-Fikr Al-Jami'i.
2. Abderrahim Sami (2019), *Cyber Attacks and Protection Methods*, Dar Al-Safwa, Beirut.

3. Abou Saada Mohammed (2020), *Information Security and Computer Protection*, Dar Al-Fikr Al-Arabi, Cairo.
4. Ahmed Fathi Soror (2019), *Cybercrime Law*, Dar Al-Nahda Al-Arabia.
5. Amr Rida Beyoumi (2002), *The Dangers of Israeli Weapons of Mass Destruction to Arab National Security*, First Edition, Dar Al Nahda Al Arabia.
6. Andy Greenberg (2019), *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*, New York: Doubleday.
7. Eric Cole, *Malware: Fighting Malicious Code*, McGraw-Hill, 2005.
8. Hazem Mohammed Atlem (2002), *The Law of International Armed Conflict: Introduction and Temporal Scope*, Second Edition, Dar Al-Nahda Al-Arabia, Cairo.
9. Michel N. Schimtt (2013), *Tallinn Manual on The International Law Applicable to Cyber Warfare*, 1st edition, Cambridge University Press, New York.
10. Mohammed Lmajdoub (2004), *Public International Law*, Fifth Edition, Al-Halabi Legal Publications, Beirut.
11. Montassar Said Hammouda (2008), *Human Rights During Armed Conflict*, First Edition, Dar Al-Jami'a Al-Jadida.
12. Mourad Fatima El-Zahra, (2021), *Information Security and Cyberattacks*, Dar Al-Yazouri.
13. Rid Thomas (2013), *Cyber War Will Not Take Place*, Oxford University Press.
14. Sameer Chopra (2021), *Cybersecurity Essentials*, Wiley.
15. Souhail Houcine El-Fatalaoui (2012), *The Customary Legal Nature of the Rules of International Humanitarian Law*, Dar Al-Thaqafa for Publishing and Distribution, Jordan.

Theses & dissertations:

1. Amani Temmuz Abderrahman El Khafadji (2023-2024), *Insurance Protection for Commercial Companies from Cyber Risks*, Master's Degree, University of Maysan, Iraq.
2. Amir El-Moussili (2020-2021), *Cyberattacks in Light of International Humanitarian Law*, Syrian Virtual University.
3. Nour Amir El-Moussili (2020-2021), *Cyber Attacks in Light of International Humanitarian Law*, Master's Thesis, Syrian Virtual University.

Articles:

1. Abdelkader Ahmed (2019), *Cyberattacks and Their Impact on Critical Infrastructure*, *International Journal of Security Sciences*, Issue 8.
2. Abderrahman Chamel Abderrahman & Zaid Lokman (2024), *The Legal Nature of Cyber Attacks in Light of International Humanitarian Law*, *Al-Noor Journal of Legal Studies*, University of Nineveh, Iraq, Volume 1, Issue of December.
3. Abderrahman Hassan (2021), *Malware and Its Impact on Network Security*, *Cybersecurity Journal*, Issue 4.
4. Amjad Abis Niama El-Fatalaoui (2016), *Cyber Attacks: Their Concept and International Responsibility Arising Therefrom in Light of Contemporary International Organizations*, *Al-Mouhakkik Journal for Legal and Political Sciences*, University of Babylon, College of Law, Iraq, Issue 4, Year 8.
5. Amira Abdeladhim Mohammed Abdeldjaouad (2020), *Cyber Risks and Means of Confronting Them in International Public Law*, *Journal of Sharia and Law*, Issue 35, Part 3.
6. Ben Guettat Khedidja (2024), *The Implications of Cyberwars for Digital Sovereignty*, *Journal of Algerian and Comparative Public Law*, Abdelhamid Ben Badis University, Mostaganem, Algeria, Volume 10, Issue 2.
7. Cherif Abdelhamid Hassan Ramadan (2021), *Cyber Warfare and its Compatibility with IHL*, *Journal of the College of Sharia and Law*, Tafahna Al-Ashraf, Dakahlia, Issue 23, Part 4.

8. Chouireb Djilali (2023), The Concept of Cyberwars and Cybersecurity, Journal of Rights and Freedoms, Amar Talji University, Laghouat, Volume 11, Issue 1.
9. Hachem Hasni Ali Kazem Helsoun (2025), The Concept of Cyber Attacks and Their Legal Nature, Journal of the Iraqi University, Volume 73, Issue 4.
10. Hamed Mohammed Ali El-Baldawoui (2022), Confronting Cyber Warfare in the Rules of International Humanitarian Law, Journal of the Iraqi University, Imam College, Issue 57, Part 2.
11. Haydar Adham Tai & Ali Mohammed Kazem (2019), Direct Participation of the Cyber Collective Authority, Journal of the College of Law, Al-Nahrain University.
12. Islam Hadib (2024), The Concept of Cyber Warfare under International Law, Defining Its Characteristics and Consequences, Journal of Legal and Economic Research, Beni Suef University, Volume 36, Issue 1.
13. M. Karrar (2023), Cyber Warfare from the Perspective of International Humanitarian Law, Nottingham University Journal of Management and Humanities, Volume 2, Issue 2.
14. Mohammad Hassan Derradji & Omar Salah Akkour (2024), Cyber Attacks According to the Provisions of International Humanitarian Law, Journal of Sharia and Legal Sciences, University of Jordan, Volume 51, Issue 1.
15. Mohammed Salah Abdel-Ilah Rabie (2024), Cyber Attacks: Between Their Legitimacy as a Means of Legitimate Defense and Their Condemnation as Unlawful Assault (An Analytical Study in Light of International Law), Journal of Legal and Economic Studies, Volume 10, Issue 1.
16. Nabila Abdelfattah Gachti (2024), Cyber Warfare and Ways to Confront It, Strategic Affairs Journal, Faculty of Law, Menoufia University, Egypt, Issue 17.
17. Nadjji Mohammed Oussama Chadli (2023), The Law Essence Journal, Tanta University, Volume 25, Issue 103, July.
18. Omar Mahmoud Amr (2019), Cyberwar in International Humanitarian Law, Studies, Sharia and Legal Sciences, Jordan, Volume 46, Issue 3.
19. Ramadan Abdallah El-Amouri (2024), Cyberwars (Reality-Challenges) in Light of International Humanitarian Law, Al-Hak Journal of Sharia and Legal Sciences, University of Bani Walid, Libya, Issue 14.
20. Saad Naceur (2021), Cyberspace Threats and the Role of Cybersecurity, Journal of Security Studies, Volume 12, Issue 2.
21. Sami Ahmed AbdelKarim (2018), Cyberwar and its Implications for National Security, Arab Journal of Political Science, Issue 60.
22. Yahia Yacine Saoud (2019), Cyber Warfare in Light of the Rules of International Humanitarian Law, Al-Mouhakkik Journal for Legal and Political Sciences, University of Babylon, College of Law, Iraq, Issue 4, Year 8.

Reports:

1. Abdessadek Adel (2009), Cyberterrorism in International Relations: A New Paradigm and Different Challenges, Al-Ahram Center for Political and Strategic Studies, Cairo.
2. Hassanin El-Mohammadi Bouadi (2005), The Invasion of Iraq between International Law and International Politics, Alexandria Knowledge Foundation.
3. International Telecommunication Union (ITU) (2022), Annual Report, Global Cybersecurity, Arabic Edition.
4. Khaled Abderrahman (2021), Cyberattacks as a Modern Tool of War, Strategic Studies, Al-Ahram Center.
5. National Cybersecurity Authority (2022), Types of Malware and Methods of Prevention, Authority Publications, Riyadh.
6. U.S. Department of Défense (2016), Dictionary of Military and Associated Terms, Publication 1-02, Joint Nov.8, 2010, as amended through Feb.15.

Websites:

1. Ali Himia (2024), Lebanese Army Officer, Legal Revisions to the Definition of Cyber Weapons, article available online: <https://www.lebarmy.gov.lb/ar/content>, accessed on 12/29/2024 at 10:00 AM).