An-Najah National University

Faculty of Graduate Studies

LEGAL RESPONSIBILITY FOR CYBER WARS IN LIGHT OF THE RULES AND PROVISIONS OF INTERNATIONAL HUMANITARIAN LAW

By
Nadia Jawad Tawfeeq Zaid Alkeelani

Supervisor
Dr. Mohammed Abu-Alrub

This thesis is submitted in Partial Fulfillment of the Requirements for the Degree of Master of International Law and Human Rights, Faculty of Graduate Studies, An-Najah National University, Nablus – Palestine.
2025

LEGAL RESPONSIBILITY FOR CYBER WARS IN LIGHT OF THE RULES AND PROVISIONS OF INTERNATIONAL HUMANITARIAN LAW

By

Nadia Jawad Tawfiq Zaid Alkeelani

This Thesis was Defended Successfully on 11/01/2025 and approved by

Mohammed Abu-Alrub Supervisor	Signature
Ahmad Abu Jaafar External Examiner	Signature
Sanaa Al Sarghali Internal Examiner	Signature

Dedication

To my beloved family,

Your unwavering support, encouragement, and understanding have been the guiding light throughout this journey. Your love has fueled my passion for research and sustained me through every challenge. This work is dedicated to you, with the deepest gratitude and affection.

To my cherished friends,

Your friendship has enriched my life in countless ways, offering laughter, solace, and inspiration. Thank you for standing by me. This dedication is a testament to our enduring bond and shared adventures.

To my esteemed colleagues,

Your collaboration, insights, and camaraderie have been instrumental in shaping this endeavor. Together, we have pushed the boundaries of knowledge and forged new pathways in our field. This dedication honors our collective efforts and the spirit of collaboration that defines our community.

May this work serve as a tribute to the meaningful connections that have sustained me along this path. Thank you for being a part of my journey.

With heartfelt appreciation

Acknowledgments

I would like to extend my deepest gratitude to Al-Najah National University for providing me with the resources, support, and guidance necessary to undertake this research endeavor. The university's commitment to academic excellence and research innovation has been instrumental in shaping my academic journey and enabling me to pursue my scholarly interests.

Additionally, I am immensely thankful to Al-Haq Institution for their invaluable assistance and collaboration throughout this master's project. Their expertise, insights, and willingness to engage us in field application have significantly enriched the quality of my work and broadened my understanding of the subject matter.

I am also indebted to the faculty members, advisors, and mentors at Al-Najah National University for their unwavering encouragement, constructive feedback, and scholarly guidance. Their mentorship has been instrumental in shaping my research methodology and refining my analytical approach.

Lastly, I extend my heartfelt thanks to my family and friends for their unwavering support, encouragement, and understanding throughout this academic journey. Your love, patience, and encouragement have been my source of strength and motivation.

Declaration

I, the undersigned, declare that I submitted the thesis entitled:

LEGAL RESPONSIBILITY FOR CYBER WARS IN LIGHT OF THE RULES AND PROVISIONS OF INTERNATIONAL HUMANITARIANLAW

I declare that the work provided in this thesis, unless otherwise referenced, is the researcher's own work, and has not been submitted elsewhere for any other degree or qualification.

Student's Name: Nadia Jawad Tawfeeq Zaid Alkeelani

Signature: Nadia Alkeelani

Date: 11/01/2025

Table of Contents

LEGAL RESPONSIBILITY FOR CYBER WARS IN LIGHT OF THE RULES AND PROVISIONS OF INTERNATIONAL HUMANITARIAN LAW

By
Nadia Jawad Tawfeeq Zaid Alkeelani
Supervisor
Dr. Mohammed Abu-Alrub

Abstract

This study addresses the legal responsibility for cyber warfare in light of the rules and provisions of international humanitarian law (IHL). It examines how IHL applies to cyber wars, highlighting the unique challenges posed by modern technological advancements and the necessity to adapt existing legal frameworks to address these challenges effectively.

The importance of this study lies in its focus on defining the concept of cyber warfare and evaluating the applicability of IHL principles in regulating cyber-attacks during armed conflicts. Despite the establishment of foundational IHL principles through the four Geneva Conventions of 1949 and the two additional protocols of 1977, the rapid evolution of technology necessitates a reexamination of these laws in the context of cyber warfare.

The research problem revolves around the lack of an integrated legal and humanitarian approach to cyber warfare, emphasizing the difficulties in comparing traditional and cyber warfare. The study adopts an analytical methodology, examining the application of IHL principles to cyberspace activities by state and non-state actors in situations that qualify as armed conflicts.

The study is divided into three main chapters:

The first chapter: explores the nature and origin of cyber warfare, its definition, and its classification within existing legal frameworks.

The second chapter: investigates how state and non-state actors engage in cyber warfare, their objectives, and the implications for international agreements and customary rules of armed conflict.

The third chapter: focuses on the legal and ethical considerations of cyber warfare, analyzing how principles like proportionality, distinction, and civilian protection apply to cyber operations.

The study concludes with a set of results and recommendations, emphasizing the importance of updating and expanding IHL to address the evolving nature of warfare. Among the most significant findings are the urgent need to clarify the legal classification of cyber warfare and the necessity for international cooperation in establishing frameworks for cyber defense and security. The key recommendations call for enhanced collaboration among states and international organizations to develop practical, enforceable measures to regulate and mitigate the risks of cyber warfare.

Keywords: legal responsibility, light, rules, provisions, international, humanitarian law

Preface

Introduction

Wars are a complex historical and social phenomenon that has significant impacts on humans and societies. Wars are generally an armed conflict between two or more groups or countries, aimed at achieving political, economic, or social interests, and are usually accompanied by destruction and loss of life. Due to technological development from the mid-twentieth century until the present time, the world has witnessed many new wars called cyber wars

This study focuses on cyber attacks carried out during or in the context of armed conflicts, which is reflected in defining known methods and means of fighting during traditional wars, and thus in the possibility of applying principles and rules of international humanitarian law to such attacks.

These attacks are known as electronic warfare, which means using computers, networks, or related systems to launch attacks on an opponent's Internet systems, property, or computer functions. These attacks can disable or destroy adversary targets, collect confidential information, or cause physical damage. Cyber weapons can be used in conflict between states, in parallel or not with traditional military warfare. Both types represent an increasing danger in the world, which threatens to become the largest international security threat.

Countries have become aware that the danger nowadays may come from cyberspace, and they must work to protect their interests. A “cyber” attack may be considered a terrorist act or equivalent to an armed attack if it is widespread, and the reality proves that a number of countries have been victims of electronic attacks to varying degrees in terms of severity and damage. Cyberspace has become a field for waging wars, just like air, space, land, and sea, using weapons that have the ability to cause extensive material damage. This technology also uses the electronic network as a means from which it can be launched and through which to carry out military operations.

Several countries have taken steps to address the legal aspects of electronic warfare both on the national and international levels. For example, the European Union took significant steps in this direction by adopting the "Cybersecurity Strategy and Draft Directive" in

2013. This strategy mainly focused on addressing cybercrime and enhancing cybersecurity within the private sector. In essence, the EU was working to create legal guidelines and regulations for dealing with electronic warfare and its associated challenges.

However, one of the most notable and successful initiatives in this field is the Tallinn Manua, which is a comprehensive document that provides guidance on how international humanitarian law, also known as the laws of armed conflict, applies to electronic warfare. It outlines the legal principles and rules governing the conduct of hostilities in the digital realm. This manual defines the role that international humanitarian law plays in regulating and mitigating the impact of electronic warfare, ensuring that nations adhere to ethical and legal standards even in the evolving landscape of cyber conflict.

Research terms and expressions

- Cyberspace is "a physical and non-physical field that includes a group of elements: computers, network systems, software, information computing, data transmission and storage, and the users of all of these elements."
- Cyberwar: The Tallinn Guide on the Applications of International Law in the Fields of Conflict and War defined it as "all cyber operations, whether defensive or offensive, which are believed to cause injury or death to humans, or damage to material objects."
- A cyberattack may occur at any time and may be the spark to start a war or a declaration of it, but if it occurs during an armed conflict, it is described as a cyberwar, as it is part of an ongoing war.
- "Cybersecurity" describes the set of tools, policies, guidelines, risk management approaches, procedures, training, best practices, assurance mechanisms, and technologies that can be used to protect the availability, integrity, and confidentiality of assets in connected infrastructures of government, private organizations, and citizens. These assets include connected computing devices, employees, infrastructure, applications, services, and communications and data systems in the cyber environment.

Research Problem

The research problem revolves around the concept of cyber warfare and the extent to which the primary rules and principles of international humanitarian law (IHL) can be applied to this new form of conflict. The main question posed by this study is: To what extent are the rules and provisions of IHL, established through the four Geneva Conventions of 1949 and the two additional protocols of 1977, applicable to cyber warfare in the context of armed conflicts?

From this main question, the study derives several sub-questions, including:

1. What is the legal definition of cyber warfare, and how does it differ from traditional warfare?
2. How do state and non-state actors engage in cyber warfare, and what objectives do they seek to achieve?
3. How can the principles of proportionality, distinction, and the protection of civilians be applied to cyber-attacks?
4. What are the legal challenges posed by modern means of warfare, and how can they be addressed through international cooperation and legal frameworks?
5. How can IHL be adapted to effectively regulate cyber warfare, given its unique characteristics and potential impact?

This study seeks to present a comprehensive and integrated legal and humanitarian approach, comparing traditional and cyber warfare while addressing the challenges posed by modern technological advancements. It aims to provide insights into how existing legal rules can be interpreted and applied to this evolving landscape of conflict.

Research questions

1. What is the nature and origin of cyber warfare, and how has it evolved over time?
2. How has the concept of cyber warfare emerged and developed in the context of modern conflict?
3. How do various actors, including state and non-state entities, engage in cyber warfare activities, and what are their objectives and motivations?

4. What are the implications of classifying cyber warfare as a means and method of warfare for the application of existing international agreements and customary rules governing the conduct of armed conflict?
5. How do legal and ethical considerations surrounding cyber warfare intersect with traditional principles of warfare, such as proportionality, distinction, and civilian protection?
6. How can states and international organizations effectively address the proliferation of cyber threats and enhance cooperation and coordination in the realm of cyber defense and security?

These revised research questions aim to provide a more comprehensive and structured framework for investigating the nature, implications, and legal dimensions of cyber warfare, while also considering its historical development and contemporary challenges?

Research Significance

This study is important from a theoretical and scientific perspective. As for its importance from a theoretical point of view, it is one of the rare studies, especially at the Palestinian level, and therefore this study is considered an attempt to contribute to supplying the legal library in Palestine. The fact that cyber wars are considered one of the modern phenomena that the world is witnessing and one of the most dangerous types of wars that threaten the security and sovereignty of countries; It requires studying ways and mechanisms to confront it from a legal perspective.

As for the scientific aspect, the importance of the research is clearly evident in highlighting the expected humanitarian impacts of the transition to the use of cyber operations in cyberspace during armed conflicts, in comparison to traditional means and methods of fighting. It is clear that this research comes in the context of the development of cyber warfare and the increasing use of technology in this field.

Moreover, it is of recent importance since cyber warfare is governed by international humanitarian laws and represents one of the main issues that determine the conditions for classifying cyber operations as part of armed conflict or even as a direct cause of armed conflict. This research seeks to ensure that the use of electronic operations during these conflicts is in accordance with international standards and laws related to this type of conflict.

Research method

Given the nature and scope of this research, it necessitates a substantial reliance on the analytical approach. This approach will be employed to assess the applicability of the general principles of international humanitarian law to the actions of both state and non-

state actors in the realm of cyberspace, particularly in cases that qualify as armed conflicts or their components.

Literature review

- **Shin (2011) "The Cyber Warfare and the Right of Self Defense: Legal Perspectives and the Case of the United States"**

The article analyzed by Shin Beomchul's research deals with an important and complex topic in the modern era, which is the issue of classifying cyberattacks as armed attacks and the resulting rights of victim states to self-defense. The research focuses on the use of force, necessity and proportionality as criteria for determining the right of states to defend against cyber attacks. My research also focuses on legal liability in cases of cyber warfare, a topic related to the legal classification of such attacks and their handling in accordance with international humanitarian laws. This topic is complementary to the article, as it addresses how to determine legal liability and legal consequences for cyberattacks and defensive actions against them (Shin, 2011).

- **Applegate (2015) "Cyber Conflict: Disruption and Exploitation in the Digital Age"**

In August of 1986, a former astronomer-turned-systems administrator, on his second day on the job, attempted to determine what was causing a 75-cent discrepancy in a UNIX accounting system at the Lawrence Berkeley National Laboratory. Clifford Stoll and his colleagues would eventually link the anomaly to a hacker in Germany who was exploiting computers to steal data from the US and sell it to the KGB in the USSR during a ten-month period (Stoll 2005). Several of the methods, strategies, and processes still employed in cyber incident response operations today were first introduced in this incident, which is among the first instances of cyber espionage. More significantly, this incident showed how nation-states or their proxies might use newly developed network technology to obtain intelligence and possibly interfere with rival governments' services and systems (Applegate, 2015).

The case of Clifford Stoll that discovered cyber espionage is one of the most significant historical examples in the development of cyber warfare. It also showcases the early form of cyber warfare strategies and at the same time emphasizes on the importance of the legal

accountability in the sphere of IHL. In his investigation, Stoll shows how nation-states, or their surrogates, could use the new network technologies for spy operations, thus sowing the seeds for future cyber warfare tactics. This case is necessary for legal regulation of the behavior of cyber operations and attribution of the responsibility for the breach of international law.

In my research, I explored the legal aspects of cyber warfare in relation to IHL and thus, the link between this historical event and my research highlights the continued need of defining and applying legal norms and rules that regulate the cyber conflict within the international legal framework.

Moreover, Stoll's experience also shows that it is necessary to recognize the dynamics of threats that exist in cyberspace, as well as threats that can lead to disruption and cause damage to civilian facilities and people. My research seeks to contribute to the ongoing discourse on how to effectively regulate and mitigate the impact of cyber warfare while upholding the principles of humanitarian law and protecting civilian lives and infrastructure from the devastating effects of cyber-attacks

- **Toure (2011) "International Response to Cyber War, Searching for Cyber Security"**

This study aims to promote the concept of global cyber peace by working on the following: examining the way ICT supports daily life, assessing cyber threats and ongoing trends, analyzing the effects of cybercrimes and cyber conflict, assessing the validity of current legal frameworks. Defining the concept of cyber peace, and establishing it as an overriding guiding principle for peaceful behavior in cyberspace, charting the course for future action (Toure, 2011).

- **Schmitt (2017) "Computer network attack and the use of force in international law: thoughts on a normative framework"**

Schmidt's research focuses on the admissibility of attacks on computer networks under the laws of war and international laws regulating the use of force in international relations. The analysis in the paper highlights several points, such as the prohibition of the use of force as enshrined in the UN Charter and the right to self-defense and concludes that traditional applications of the prohibition of the use of force may fail to adequately protect

shared societal values threatened by computer network attacks. While my research focuses on legal liability in cases of cyber-attacks and analyzing it within the framework of international humanitarian law. It discusses the laws and provisions that regulate the legitimate use of force and response to cyber-attacks, and works to provide an alternative normative framework based on assessing the consequences resulting from these attacks (Schmitt, 2017).

It is noted that there is a similarity between the two papers in their focus on the acceptability of the use of force in confronting cyber challenges, but the two papers differ in the approach taken to provide solutions. While my research proposes an alternative normative framework based on consequence analysis, Schmitt's research is based on reconsidering traditional applications of the prohibition on the use of force.

- **Hughes (2010) "A treaty for cyberspace"**

The article explains why it could be time for international society to start ratifying a worldwide cyber treaty. It starts with going over the merging factors that have made cyberspace a vibrant arena of state-to-state political and economic rivalry. The main arguments about whether or not cyberwarfare fall under the purview of the laws of armed conflict are then examined. The article's conclusion makes the case that, with the right political backing, a multilateral cyber treaty could be a useful tool for preventing states from using cyberspace as a default forum to settle disputes outside the purview of customary international law and diplomacy (Hughes, 2010).

- **Smith () "The New Law of War: Legitimizing Hi-Tech and**

Infrastructural": This article looks at how recent developments in strategic theory and a new generation of high-tech weaponry have altered the interpretation of the humanitarian norms of war. Humanitarian law is being used more often than ever to give military action legitimacy-far from going out of style (Smith, 2002).

- **Schmitt (2002) "Warfare by Networks: Attacks on Computer Networks and Law in War"**

Information warfare was introduced to revolutionize armed conflict. Computer attack is any process aimed at disrupting, preventing, weakening or destroying information

contained in computer networks. This article examines the use of these attacks in international armed conflict, where their consequences can be far-reaching. The article begins with an analysis of the applicability of international humanitarian law to attacks using computer networks, and then moves on to examine the legal impact of this legal system on the use of these attacks as a means of war (Schmitt, 2002).

Chapter One

The concept of cyber wars

Prohibiting the use of force in international relations is considered a basic principle in international law, and it is the point imposed by the main articles and internationally recognized laws. This principle manifests itself as an expression of the commitment of all states to control and use force wisely and deliberately and not to threaten or use it in any context that might involve a violation of the territorial integrity or political independence of others.

The United Nations Charter was particularly keen to promote and consolidate this principle. This is clearly demonstrated in the fourth paragraph of Article II of the Charter, where members of the United Nations are strictly prohibited from threatening or using force in their international relations, unless doing so is consistent with the aims and purposes of the Organization (*United Nations Charter*, 1945). It stipulated that "all Members of the Organization shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations."

This is what was enshrined in the first rule of the Tallinn Manual on International Law Applicable to Cyber Warfare (Schmitt, 2013), which states that "a State may exercise control over cyber infrastructure and its activities within its sovereign territory." In addition, Rule (10) of the same manual prohibited the threat or use of force and considered it illegal, stating that "a cyber operation involving the threat or use of force against the territorial integrity or political independence of any State, that is, a cyber operation that is otherwise inconsistent with the purposes of the United Nations, shall be deemed illegal" (Schmitt, 2013).

This text represents a strong affirmation of the international commitment to control the use of force and not to infringe on the sovereignty of other countries. It should be noted that this principle was not established easily but rather came after many years of conflicts and wars that caused enormous damage to humanity and burdened countries with devastating burdens, which made the need to establish it to achieve international stability urgent. Many international and regional declarations and agreements, in addition to global charters, are among the mechanisms that affirm this principle and specify the

circumstances in which the use of force can be resorted to,[1] provided that this is in accordance with certain conditions and specific controls, and in exceptional cases that are consistent with the principles and objectives of international law.[2]

Although international laws strictly prohibit the use of force as a means of resolving disputes between states, this has not prevented the development of new forms of conflicts and attacks. Instead of relying on traditional wars that include the use of direct military force, countries have begun to move towards developing their military capabilities and diversifying their methods to confront new threats, including cyber-attacks.

Rule (30) of the first edition of the Tallinn Manual defines a cyber-attack as "a cyber-operation, whether defensive or offensive, that is likely to cause injury or death to persons, or damage or destruction of facilities." (Schmitt, 2013, p. 7)

The development of cyber-attacks comes as a result of the tremendous scientific and technological development that humanity has witnessed, as countries and non-international groups have become able to use technology to carry out attacks directly or indirectly. Consequently, cyber wars began to appear as a feature of modern wars, as cyberspace is harnessed in the military field to use modern technologies in managing operations and attacks during conflicts (Saud, 2018).

Indeed, cyber wars have become a major challenge in the modern era, as conflict relies on technical and software mechanisms rather than traditional military force. This reflects the transformation witnessed in the nature and methods of wars, and opens the door to new challenges faced by specialists in the field of international law (Hathaway et al.,

[1] The United Nations approach to the above-mentioned has been emphasized in many international declarations and charters, including:

- Paragraph (13) of the first section of the Manila Declaration of 1982.

- Article (5) of the Charter of the League of Arab States of 1945.

- Article (2) of the Bogota Charter issued on 4/30/1948.

[2] Among these exceptional cases, we mention:

- The state of collective security, and we find its legal basis in Chapter VII of the United Nations Charter (Articles (41, 42), with the aim of maintaining international peace and security and protecting the interests of the international community.

- The right of legitimate defense, which is stipulated in Article (51) of the United Nations Charter.

- International humanitarian intervention: which is carried out through a decision of the Security Council in cases where acts of repression and violence occur against many countries.

- Exercising the right to self-determination: which is confirmed by Article (4) of the Third Geneva Convention relating to prisoners of war of 1949.

2012), especially in understanding the nature of these attacks and identifying their elements. The challenge is not limited only to that but also relates to the scope of these attacks in the context of international humanitarian law, and the international and criminal liability consequences that may result from them, whether these consequences relate to civil or criminal liability.

In this regard, we note that cyber wars can be included within what is prohibited by the text of the fourth paragraph of the text of Article Two of the United Nations Charter, in addition to a group of international agreements and treaties, especially the Geneva Conventions of 1949, which are applied during periods of armed conflict, and other international agreements that can be relied upon to prohibit this type of war and cyber-attacks, then came the Tallinn Declaration, which represents a reflection of the provisions and rules of international law in general and international humanitarian law in particular, but in the virtual or electronic world.

During this requirement, the researcher will clearly define the concept of cyber wars, distinguish them from other concepts associated with the illegal use of cyberspace, and explain the legal basis for cyber wars. This is as follows:

1. The concept of cyber warfare

Cyberspace in general refers to a physical and non-physical domain consisting of a variety of technical elements, such as computers, network systems, software, and information computing, as well as the transmission and storage of data and information, and also the users who interact with these elements (Schmitt, 2017). Cyberspace is considered an open field that is difficult to control due to its great complexity and multiple ramifications.

With the development of technology and the spread of the use of the Internet and smart devices, the risks and threats associated with cyberspace have increased. These threats include cybercrime, cyber-attacks, cyber espionage, cyber terrorism, and cyber hacking. In addition, cyberspace has become an arena for cyber warfare, a concept that refers to military operations conducted over the Internet and targeting electronic systems and networks (Lin, 2012). Given this growing challenge, researchers and experts in international law, as well as states and international organizations, have begun working to understand and address this evolving type of warfare. These efforts aim to establish

mechanisms and controls to ensure that these operations are conducted in accordance with the rules of international law and to ensure stability and security in cyberspace.

Firstly, it should be noted that the term cyber war has a specific meaning that differs from the term cyber-attack or cyber-attacks launched by one country against the electronic systems of another country.

According to the definition of Michael N. Schmidt a cyber-attack means those actions taken by a state with the aim of launching an attack on the enemy's information systems, with the aim of influencing them and defending the information systems of the attacking state (Schmitt, 2017). If cyber-attacks turn into armed conflict, it is called "cyber war" or cyber-attack according to the laws of international humanitarian law, where cyber conflict, whether offensive or defensive, is expected to lead to injury or killing of individuals, or cause damage to property. Thus, the scope of cyber-attacks expands to include broader aspects of cyber wars and may occur outside the contexts of armed conflicts and are considered a reason for the beginning of the conflict (Hathaway et al., 2012, p. 833).

Schmitt sets out five main criteria for qualifying a cyber-attack as a use of force: severity of the damage; immediate subsequent damage; a direct link between the armed force and its consequences; the cyber-attack crossing international borders; and finally, the ability to assess or distinguish the physical act (Schmitt, 2017).

Cyber-attacks are also defined as a series of actions carried out by parties involved in an armed conflict with the aim of gaining a tactical or strategic advantage in cyberspace. These attacks include the use of technical and information capabilities to damage or disable an opponent's computer systems, or even for the purposes of espionage to obtain confidential information (Nacib, 2021, p. 222).

Cyber-attacks are characterized by being carried out indirectly, as the primary goal is to influence the military, economic, or political ability of the enemy by targeting their electronic systems. These attacks range from instantly destroying computer infrastructure, disrupting vital services that rely on the Internet, or even accessing sensitive information for intelligence gains. Cyber-attacks are mainly used in the context of armed conflicts that escalate to the level of war, where they have a significant impact on the military and security strategies of the countries involved. It is considered one of

the modern tools of war that countries seek to develop and develop their capabilities in, given its increasing importance in the current digital age (Gervais, 2012).

It is important to note that cyber war is distinguished from traditional wars in several aspects. The concept of traditional war includes the use of organized forces, a clear declaration of the state of war, and the definition of the battlefield, while cyberspace attacks appear to have an undefined scope and carry vague goals, as they travel through information and communications networks that cross international borders. In addition to this, they use what can be described as new electronic weapons that suit the nature of the electronic race in the information age, as they target vital installations or are hidden by agents of the intelligence services. Depending on the nature of the weapon used, a criterion can be used to distinguish between cyber warfare and conventional warfare, as the former is considered a war in which non-conventional weapons are used that cause widespread destruction (Bayoumi, 2012, p. 25).

Despite differences in definitions, cyber-attacks can be considered part of cyber warfare if they are used within the context of an armed conflict and aimed at achieving military objectives. Accordingly, cyber warfare can be defined as a set of actions taken by parties to an armed conflict to gain advantage over their opponents in cyberspace by using various technological tools and technical people. These actions can achieve various military objectives, such as disabling, destroying, or usurping enemy computer systems, obtaining classified information from the enemy, or influencing public opinion in favor of the attacking party (Lin, 2012, p. 515).

In 2007, cyber-attacks were defined by the United States Strategic Command as “the US Strategic Command’s adaptation of computer system operations with the aim of preventing enemies from effectively using it, in addition to preventing infiltration into information systems and communication networks for the purpose of collecting, detaining, and analyzing the data contained therein.” It is noted that this definition is in line with Article 5 of the Council of Europe Convention on Cybercrime, which states: “Each State Party shall adopt the necessary legislative and other measures to criminalize in its national law the following act, if it is committed intentionally and unjustly: “Seriously obstructing the operation of a computer system by entering, transmitting, destroying, deleting, corrupting, altering or destroying computer data ("Convention on Cybercrime," 2001, p. Article 15).”

It is clear from the above that there is a close link between cyber-attacks and cyber warfare. Some military objectives have been identified for cyber warfare, such as disrupting enemy computer systems and obtaining secret information. While the definition of the US Strategic Command, as well as the Council of Europe Convention, refers to preventing intrusion into information systems and communication networks, and collecting, seizing and analyzing data, which are specific military objectives of cyber warfare. The seriousness of cyber-attacks and their impact on the national security of countries was emphasized. The definition of the US Strategic Command and the Council of Europe Convention also indicate the necessity of criminalizing these attacks, which emphasizes their seriousness and the need for international cooperation to combat them.

1.1. Types and levels of cyber warfare

The importance of cyber warfare is increasing significantly with the tremendous developments in information technology that affect the nature of conflicts and conflicts between countries. States' pursuit of cyber power constitutes a major shift in the character of conflicts. This pursuit opens the door to a deeper understanding of the phenomenon of the emergence of hostile electronic activities, and reveals the complexities of cyberspace interactions. On the one hand, cyber security, both at the state level and at the global level, is greatly affected by such wars. On the other hand, the levels of cyber wars differ depending on the parties' participation in them and the participation of these parties in these hostile actions. In this section, we will focus on the further elaboration of the level of cyber warfare and its consequences (Alsaade, 2022).

1.1.1. Personal information war

Personal information warfare is a process in which some individuals break into networks or electronic devices with a view of stealing information stored in the devices. It is this information that is very often of paramount importance, military, economic, industrial, or commercial, which entails significant strategic consequences for the party targeted (Shafiq, 2016). This kind of attack seeks to gain unauthorized access to electronic systems to get access to information that may include personal details, business data, and even national security information. The reasons for cyber spying are numerous and are comprised of theft, espionage, sabotage, and blackmail. Their objectives are accomplished through various methods including malware attacks, social engineering, brute force attacks, and denial of service attacks (Aleisaa & Enab, 2019).

The warfare of personal information harms individuals and organizations in society. The loss of financial information may lead to loss of money while identity theft may lead to the development of false identities which are used in different criminal activities. Privacy invasion also has a high potential of endangering people besides the harm that may be inflicted on the image of individuals or organizations due to the spread of wrong information.

Due to the fact that these attacks are capable of causing huge losses in a short span of time, most countries have learned to rely on them in their efforts to achieve certain goals, especially during periods of political unrest with other nations or during wars and other forms of militancy. For instance, in a report of an investigative committee formed by the European Parliament in 2001, the United States is said to be involved in an electronic espionage network known as the "Echelon network" that was formed during the Cold War for espionage and stealing of industrial information from Europe (Aleisaa & Enab, 2019).

However, it is worth stating that states are not the only targets of these attacks. Cyber espionage also targets commercial and advertising companies as well as non-governmental organizations.

1.1.2. Information war between companies and institutions

Information war between companies and institutions is a phenomenon that expresses the intense competition that takes place within the framework of commercial and economic business. This type of conflict seeks to gain an upper hand in an organization or business by seeking access to privileged information or by integrating artificial intelligence and data analytics to inform decisions. This conflict is centered on obtaining competitors' secretive and privileged data and employing it fraudulently to gain more clients or tarnish competitors' image in the market (Al-Basha, 2001).

In turn, information warfare activities are manifold, and the following methods are used: gaining access to the competitors' information systems to steal valuable information, including results of scientific and experimental research and development, and business plans, and using these data to cause more significant damage to the opponents. Some of the information warfare tactics also include the use of malware or viruses that are used to destroy data structures as well as injure important systems belonging to the competitors.

In general, information warfare is a multifaceted process that poses new challenges and calls for new approaches and legislation that would regulate information operations, restrict the violation of privacy rights, and protect personal data, as well as improve cyber security to prevent unlawful cyber-attacks.

1.1.3. Global information war (cyber war)

Cyber war or electronic warfare can be described as a particular kind of conflict that takes place in cyberspace where electronic tools and weapons are used in offense and in defense. In this regard, attacks are chiefly aimed at computers, the enemy's electronic networks, or state-operated electronic systems that store some critical data. These attacks are conducted with the intention of degrading the opponent's ability to operate and gain value from such systems, devices, and networks or even destroying them. This may involve computer espionage and hacking of important computer networks with the aim of acquiring secret information, or the use of viruses and malware to jam computers and networks (Shafiq, 2016). The cyber warfare techniques also involve using phishing, and people are lured to open the link or download an infected file where the attacker gains unauthorized access to the victim's systems and can manipulate information.

Cyber wars are a great obstacle to the safety of states, organizations, and institutions because cyber-attacks can cause catastrophic damage from loss of data or disruption of essential services and may even affect national security. Thus, the response to this kind of threat must be on an international scale, adding further rigidification to cyber security and legislation in terms of data prevention as well as law enforcement.

In addition, these wars are part of international conflicts and economic competition, and their goals are to influence the interests and policies of other parties by obtaining and controlling information. The countries that enjoy enhanced information technology technologies have a strategic edge in these types of conflicts whereby they can apply noble systems and also make precision electronic attacks. Developed countries have the capability of defending vital and important infrastructure, as well as their capacity to control electronic networks that will not open the door in front of cyber-attacks at any time. But modern developments in information technology allow enemies to be addressed in different ways, whether on an individual basis or a state or institutional basis (Al-Hamdan, 2016).

In general, there are three main levels of cyber warfare, and these are important concepts that are central to defining the nature of this warfare. The first level of cyber warfare is the operations that are related to traditional wars, and it is used to gain cognitive and strategic advantage. For instance, an air defense system can be assaulted in a manner that causes many losses in terms of human lives, which are crucial in the ability of a state to protect itself, making them very vital in the context of national security. The second level is limited electronic warfare, where infrastructure and civilian targets are directly targeted. The main objective at this level is to cause damage to the community's infrastructure and basic services, thus reducing the state's ability to respond and withstand. The third level refers to unlimited electronic warfare, where the focus is on achieving comprehensive destructive effects on the infrastructure and society as a whole. The goal is to disrupt normal response capacity and inflict maximum physical and economic losses. Attacks at this level can include targeting capital markets and critical infrastructure such as power generators and electrical grids, causing significant disruption to economic and social life (Aleisaa & Enab, 2019).

It must be noted that cyber-attacks usually target specific information or information systems of the target party, for various reasons related to increasing the value of that information or reducing its value to the attacker or the defender, or to both together. The importance of information and its systems is measured by the extent to which the attacker or defender acquires it, as the value of this information constitutes the main indicator of the goals that the attacker seeks to achieve.

The goals of cyber-attacks vary greatly, and these goals may often be financial endeavors, such as stealing and selling bank account records, where the attacker aims to obtain financial gains through illicit means. The goals can also be political or military, as the attacker seeks to influence the military policies or strategies of the targeted country. In addition, cyber-attacks may have goals related to arousal and demonstrating technical capabilities or the ability to influence, as occurs in the cases of hackers who use their skills to penetrate systems for illegal purposes or to show off their technical skills. These diversities in the goals of cyber-attacks reflect the complexity of the current cyber context and highlight the importance of studying this phenomenon carefully to understand the motives and effects of these attacks at various levels, whether economic, political, or social (Aleisaa & Enab, 2019).

Chapter Two

Legal adaptation of cyber warfare

Cyber wars are distinguished from traditional conflicts in several aspects. In the traditional context of warfare, there is the use of standing armies and a clear declaration of the state of war with a clear delineation of the battlefield. In contrast, cyberattacks appear indefinitely in space and are ambiguous regarding targets. These attacks are carried out across information and communications networks that cross international borders. It is characterized by its reliance on new electronic weapons that suit the electronic race in the information age. These attacks are directed towards vital installations or are carried out by agents of intelligence services, and therefore, distinguishing cyber warfare from traditional warfare depends largely on the nature of the weapon used (Saud, 2018). Examples of cyber operations include espionage, identifying targets, and information operations to influence the enemy's morale and will to confront combat. It also includes operations to disrupt, distract, or interfere with enemy communications systems to disrupt force coordination. The concept of cyber warfare shows that it not only targets military capabilities and systems, but may also target the critical infrastructure of society (Gisel et al., 2020).

The use of cyber operations has become a reality in armed conflicts, with the first cyber-attacks carried out during the Kosovo War in Yugoslavia (Al-Fatlawi, 2016). Some countries have acknowledged implementing cyber operations in their conflicts, such as the United States, the United Kingdom, and Australia. These operations target vital infrastructure and affect countries involved in conflicts, as happened in Georgia in 2008 and Ukraine in the period between 2015 and 2017. American intelligence reports also confirmed in 2009 that some armed groups, during the occupation of Iraq, had hacked websites that received very important data transmitted by drones to determine the movements of these groups, which helped the latter monitor American military movements directed against them(Al-Fatlawi, 2016).

Cyber-attacks are accelerating and expanding at an alarming rate, with serious impacts on humanity, which imposes the need to search for a legal framework that regulates these attacks in light of the existing legal vacuums. This part of the study aims to review the issue of the extent to which international humanitarian law matches the reality of cyber-attacks. To solve these challenges, we will first analyze the adaptation of cyber-attacks

under general international law and then address their adaptation under international humanitarian law.

2. Adapting cyber-attacks to international law

International law has not explicitly addressed the issue of cyber-attacks, especially in peacetime, partly due to the relatively recent use of Internet networks. The rules of international law related to international relations were developed before the emergence of cyberspace, and therefore these rules may not be appropriate for modern technologies in the field of warfare. As cyberspace becomes more widely used as a space for conflict between states, threats to international peace and security have increased. In the absence of specific legal provisions in public international law relating to these attacks, we must explore the issue of adapting them in accordance with the basic principles of public international law, which include the principle of sovereignty and the principle of the prohibition of the use or threat of force.

2.1. The principle of prohibiting the use of force

As for the principle of prohibiting the use of force, cyber-attacks and the principle of prohibiting the use of force and the threat of its use are considered a starting point for traditional international law, which is based on the principle of equality in the exercise of absolute sovereignty without restrictions. These concepts have contributed to the emergence of several conflicts and wars, leading to chaos and instability in international relations. After the two world wars, the necessity of prohibiting wars as a means of settling international disputes was confirmed, which prompted the establishment of the United Nations with the aim of maintaining international peace and security as Article 2, paragraph 4, of the Charter of the United Nations proclaims.

Article (4/2) of the United Nations Charter also establishes a major principle of public international law that all members in their relations must eliminate the threat or use of force against the territorial integrity or political independence of any state, or in any other situation inconsistent with the principles of United Nations".

There is no doubt that the location of this article in the International Charter, and the linguistic structure it adopted, indicates its importance and prominent role in achieving a comprehensive vision for the United Nations in building and strengthening international peace and security, by strengthening the principles based on not threatening or using force

(Samoudi, 2018, p. 339). Therefore, the point of view adopted regarding this article comes within the framework of establishing a general prohibition on the use of force or the threat thereof in the context of relations between states. This principle has witnessed development to make it a recognized international custom, as confirmed by the International Court in the case of "military and paramilitary activities" against Nicaragua in 1986. The International Court of Justice's advisory opinion on the legality of the threat or use of nuclear weapons stated in Article 2, paragraph 4, of the Charter prohibits the use of force regardless of the weapon used. However, there is still no global consensus on the precise point at which cyber-attacks can be considered a use of force under Article 2, paragraph 4, of the Charter ((ICJ), 1986).

Article 51 of the International Charter stipulates that nothing weakens the individual or collective right of states to self-defense in the event of armed attack. This article raises some questions regarding the discrepancy in the terminology used. While Article (51) refers to the requirement of armed assault as a condition for activating the right to self-defense, Article (4/2) refers to the prohibition of the use of force or the threat thereof.

These two articles can be interpreted in different ways, resulting in different legal options for countries under attack. For example, when a state is subjected to armed attack, it can use force to defend itself, whether individually or collectively, as stipulated in Article 51 of the Charter. However, when there is a use or threat of force, without it reaching the level of an armed attack, the affected state faces different legal options. This action can be a counter-reaction, giving the affected state the ability to respond by other means without resorting to the use of force (Elagab, 1986, p. 29; "Gabčíkovo-Nagymaros Project (Hungary/Slovakia)," 1997, Para. 71).

On the other hand, the idea of countermeasure as an option before the aggressed state stipulated in Article (22) of the Draft Articles on the Responsibility of States for Unlawful Acts of 2001 was restricted by a set of conditions, the most important of which is the requirement of proportionality between the breach and the corresponding breach, and this is what the International Court of Justice affirmed in Kosovo case in 1997 ("Gabčíkovo-Nagymaros Project (Hungary/Slovakia)," 1997, Para. 71).

In addition, the term "force" in the Charter includes all forms of force without specifying its type, which includes threats regardless of the means used. Strong interference includes

various forms, including military, financial, and sabotage intervention, whether individual or collective, explicit or disguised, and interference through cyber-attacks is one form of this interference.

Technological advances in the electronic field have led to the emergence of new concepts, including the concept of "cyber power." Superiority in the electronic field has become vital for carrying out effective operations in various fields by using cyber power to influence technological command and control systems. A distinction must be made between the use of cyber-attacks for military purposes and traditional attacks, as the former primarily targets military infrastructure and military information security, while the latter targets non-military objectives such as information wars, spreading rumors, and illegal financial transfers (Al-Dulaimi, 2018).

Here, Rule (31) of the Tallinn Manual indicates that the principle of distinction applies to cyber-attacks. This rule represents a true reflection of the principle of distinction that must be adhered to between warring parties under the provisions and rules of international humanitarian law, especially the text of Article (3) of the Hague Regulations relating to the Laws and Customs of War on Land of 1907, as well as Common Article 3 of the Geneva Conventions, as well as the text of Article (4) of the Fourth Geneva Convention, which defined who civilians are, as well as the text of Article (43/2) of the First Additional Protocol of 1977.

Article 4/2 of the United Nations Charter also refers to the criterion for adapting cyber-attacks based on their effects and the resulting damage, without regard to the means of implementation used((ICJ), 1998, p. 2016). The International Court of Justice confirmed this concept in its Advisory Opinion on the Legality of the Threat or Use of nuclear weapons. Emphasizes that law enforcement must take into account the unique characteristics of nuclear weapons, such as their destructive potential and their ability to cause untold pain to humanity and harmful impact on future generations.

In addition, Article 4 of the Charter prohibits any use of force, regardless of the means used. In this context, some countries have confirmed that exceeding the limit of use of force does not depend only on digital means, but also depends on the effects of cyber-attacks. Thus, a State carrying out a cyber-attack against another State is considered a violation of the prohibition on the use of force if its effects are similar to or exceed those

resulting from the use of conventional weapons (Schmitt, 2013, Commentary on Paragraph 1 of the Explanation of Rule 69 of the Tallinn Manual), and the provisions of international humanitarian law relating to the protection of persons and property during armed conflicts apply in this case.

Returning to the third section of the Tallinn Manual (Rules 32-36), we find that attacks against civilians are prohibited, and the fourth section of the same manual (Rules 37-40) prohibits attacks against civilian objects. These two sections of the Tallinn Manual represent a true reflection of the requirements of the Fourth Geneva Convention relative to the Protection of Civilians of 1949.

Based on what was mentioned, the concept of force referred to in Article 2, Paragraph 4 of the United Nations Charter includes large-scale cyber-attacks targeting civilian populations during or outside conflicts. The shutdown of computers that control water stations and dams, or the occurrence of fatal and intentional engineering accidents, such as computers directing incorrect information to aircraft or the collapse of nuclear power plants, are considered dangerous cyber-attacks, and their effects go beyond traditional wars. Rule (38) of the Tallinn Manual clarified what is meant by civilian objects: "Civilian objects are all objects that are not military objectives," and Rule (37) prohibited targeting anything that is not military, stating: "Civilian objects may not be the target of cyber-attacks." Serious cyber-attacks are considered an armed attack even if no people are injured, compared to traditional attacks that may not cause injuries or property loss. It is emphasized that States are bound by responsibility in accordance with Article 4, Paragraph 2 of the United Nations Charter, if cyber-attacks lead to tangible physical effects on civilian or military objects (Shin, 2011, p. 111).

In addition, the International Court of Justice showed in the case Nicaragua v. United States of America (1986) that Article 51 does not refer to specific weapons, and the concept of weapons can be applied to any use of force regardless of the means of implementation. Although cyber-attacks may not use conventional weapons, this does not necessarily mean that they are not armed. The use of any device that causes significant loss of life or extensive destruction of property is considered to meet the requirements for an armed attack. The International Court of Justice confirmed that the right to self-defense applies to cyber-attacks, as NATO had already demonstrated in its response to the Estonia attacks in 2007, where cyber-attacks were considered an armed threat that included all

NATO members (Al-Fatlawi, 2016, p. 624). The information in the Tallinn Guide, issued by the International Committee of NATO in 2013, confirms that the use of actual military force can be justified in the event of a cyber-attack that results in human casualties (Schmitt, 2013, Chap. 14).

2.1.1. The principle of sovereignty

Cyber-attacks are one of the modern and widely used means of resolving conflicts between countries, due to their speed, ease of use, and low cost. A state can simply disable another state's military or civilian facilities and infrastructure, allowing them to be taken over without having to use conventional means of warfare. The idea of sovereignty is linked to the early emergence of the state and the organization of international society, and the Treaty of Westphalia in 1648 laid the foundations for this concept Sovereignty had several evolutions to fit the new environment, as sovereignty was not only associated with political implications of the state's ultimate power within its territory but also its autonomy from other states (Al-Ghunaimi, 1993, pp. 319, 322).

As a legal term, the concept of sovereignty "means the legal capacity of the state and determines its identity from other persons in international law" (Al-Ghunaimi, 1993, pp. 317-318). Sovereignty enables the state to exercise its powers internally and externally and to rule its business free from external control. This principle represents "the cornerstone of international law," which has been recognized and concretized in the United Nations Charter by finding in its text the only principle attributed to the principle of sovereign equality between all its members (*United Nations Charter*, 1945, Art. 2, Para. 1).

Considering the situation connected with the definition of the term "use of force" provided in Article (4/2) of the United Nations Charter, and the absence of the meaning of this term in international agreements or international custom. This case poses great analytical difficulties in the issues of international rights and duties in the sphere of international defense and security. If we turn to the Tallinn Guide, we will see that it states that any aggression against a state, including cyber aggression, is regarded as an infringement of the sovereignty of the attacked state and this means that the latter has a right to respond to this aggression. This response is seen as a prerequisite, that is, the size and impact of the attack must be within a certain range. This scope is still being actively

studied by experts, and in order to define it, there is a set of characteristics that have to be present in wars or cyber-attacks in order to be considered as an armed attack. This work will therefore seek to explain the legal basis upon which the attacked state can invoke Article 51 of the United Nations Charter and respond to attacks.

Such actions speak of the necessity of creating an international context that would help in the enhancement of the comprehension of legal notions and the actual fight against contemporary threats to security, such as cyber threats, which are becoming more diverse and innovative. Thus, this work helps to contribute to the goals of the International Charter and the maintenance of international peace and security, as well as the recognition of states' rights to protect themselves from possible threats.

Sovereignty is no longer solely a political and legal concept, but it is also a concept that changes with technology and the appearance of cyberspace. The term cyber-sovereignty is used, which means that the state sovereignty and judicial regulation of the space of cyberspace are connected with the concept of cyber security. Cyber security is also considered the technical and administrative measures to safeguard digital space and information. Cyber sovereignty is closely connected with the concept of cyber security,[1] where security refers to the protection of the infrastructure linked to the Internet, while sovereignty is about information and content in cyberspace as part of sovereignty (Cheraitia, 2020, p. 404).

The possession of cyber-power by states has turned into a bigger threat to the sovereignty of targeted states in the military, economic, cultural, and political domains. Cyber-attacks are a violation of cyber sovereignty, and target the Internet infrastructure, digital systems, and communications, which is considered a threat to the state's sovereignty in the digital space. The concept of cyber sovereignty includes the right of a state to independently manage its own network on the Internet and to monitor bodies, institutions and activities within its territory in accordance with international law. Any infringement of the electronic infrastructure is considered a violation of sovereignty, and the principle of sovereignty obligates states to prevent the use of their electronic infrastructure for

[1] Rule (4) of the Tallinn Manual referred to the sovereign immunity of states and the inviolability of attacks on them, stating: "Any interference by a state in the cyber infrastructure, on board a platform enjoying the sovereign immunity of another state wherever it is located, constitutes a violation of the principle of sovereignty," p. 2.

activities that target the cyber-sovereignty of other countries.[1] Cyber-attacks pose an unlawful international threat, and thus protecting commercial and civil activities is essential for future national security.

2.2. Adapt cyber-attacks in accordance with international humanitarian law

International humanitarian law, also referred to as jus ad bellum or the law of armed conflict comprises a body of international legal principles designed to limit the use of force in times of armed conflict and safeguard civilians and non-combatants from its hazards. Its primary objectives include ensuring the humane treatment of individuals detained by parties to a conflict, including prisoners of war, by guaranteeing their basic needs are met. Additionally, it seeks to protect civilians by prohibiting their direct or indirect targeting and providing measures to shield them from the perils of combat. In addition, international humanitarian law has the objective of protecting property from the negative impacts of conventional armed conflict. It achieves these goals by regulating the use of force, governing military conduct, and delineating the obligations that parties to a conflict must adhere to.

The provisions of international law have been compiled to include the criminalization of war but at the same time acknowledge that there are circumstances where force can be used. However, this does not exclude military operations or internal conflicts in countries from happening. Much has been done to prevent armed conflicts and to establish the principles of conducting military operations in order to minimize the adverse impacts—or the effects that impact non-combatants. These efforts have led to consensus on a number of legal norms, or the rules of international humanitarian law, that are binding on all parties to an armed conflict (Verri et al., 1988, p. 49).

The four Geneva Conventions of 1949 and two protocols of 1977 are the main sources of rules of international humanitarian law. They also prescribe the rights of persons who do not take part in combat and designate the way of treating them, as well as the rules for protecting civilians and their property in the course of military operations. Thus, with the change in the nature of wars, the evolution of technology, the complexity of weapons, and the diversification of their application, there was a continuous need to modify and

[1] Rule (5) of the Tallinn Manual states that "A State shall not allow its knowledge of the use of cyber infrastructure located on its territory or under its exclusive governmental control to be used for acts that adversely and unlawfully affect other States", p. 2.

supplement international humanitarian laws to make them effective. The immense advancement in science by the countries which was utilized to build up the military strength made it mandatory to regulate all these changes and developments under legal control and demarcate the extent to which all the parties involved in the conflicts should go. This is what international humanitarian laws aim to achieve since they are always in the process of updating themselves and adjusting their rules to the new trends in the military domain and its evolution.

In addition, the use of cyberspace in the military field is considered an important development that opens the door to new conflicts that may arise there. This development is also considered a model of the transformations that resulted from the development of information technology, as this technology has become an integral part of the management of military forces in the areas of command, control and logistics, in addition to accurately directing weapons to achieve maximum possible effectiveness and reduce collateral damage. This use also facilitates the coordination of movements and actions of military forces through communication networks that allow the exchange of information and images on the battlefield on a large scale (Lin, 2012, p. 516).

But this increasing use of cyberspace for military purposes has raised debate about the extent to which the laws of international humanitarian law apply to what might be called cyber war. In the absence of explicit documentation in international humanitarian law conventions that addresses this advanced type of operation, the debate continues about the extent to which traditional laws of war include these new and advanced activities in the cyber domain.

Before examining the extent to which the articles of international humanitarian law apply to cyber operations, it must be noted that international humanitarian law applies when an armed conflict erupts, as stipulated in Common Article 2 of the Geneva Conventions of 1949, stating that “these Conventions apply in the event of armed conflict between the High Contracting Parties, even if none of them recognizes a state of war.”. Accordingly, the question arises as to whether the rules of international humanitarian law should be applied to cyber operations alone, without them being part of conventional military activities.

In the first requirement, I will clarify whether cyber-attacks are adapted as armed conflict.

2.2.1. Adapting cyber-attacks as a form of armed warfare

The prevalence of cyberattacks and their classification as part of armed conflicts is an issue of great importance, especially when it comes to the application of international humanitarian law.

We must first point out that the issue of applying international humanitarian law to cyberattacks is a subject of widespread controversy in international discussions, and this is evident through the efforts being made by the open working group established by the United Nations among its members, with which a group of government experts participated. These two teams are tasked with studying how international humanitarian law applies to the use of technology in the field of information and communications.[1] During the years 2013 and 2015, the member states of the Intergovernmental Group-the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security-reached, in a report by the Secretary-General, an agreement that the provisions of international law, including the Charter of the United Nations, can be applied in the context of information and communications technology. This agreement underscores the importance of adhering to international legal principles, which include the principles of humanity, necessity, proportionality, and distinction.[2] Based on these principles, cyber-attacks can be classified as part of cyber conflicts, especially if they are used to achieve military objectives within the context of armed conflict (Saud, 2018, p. 85).

We find that the Tallinn Manual contains a rule that confirms the applicability of the provisions of the law of armed conflict to cyber wars, which is Rule (20), which states: "Cyber operations carried out in the context of armed conflict are subject to the law of armed conflict."

The guide stressed the necessity of applying the principle of distinction to cyber wars, which is Rule (31), which represents a true reflection of what is included in the provisions

[1] United Nations General Assembly Resolution No. 27/73 "Developments in the field of information and telecommunications in the context of international security" United Nations 73/27/A/RES, December 11, 2018, paragraph 5; And United Nations General Assembly Resolution No. 73/266.

[2] UN General Assembly Resolution "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General" UN Doc. 174/70/A, 22 July 2015, paras. 24 and 28 (d).

and rules of the law of the war and international humanitarian law as a common principle of the Hague Conventions, the Geneva Conventions, and the First Additional Protocol to the Geneva Conventions.

The guide also emphasized the principle of military necessity and proportionality, as Rule (14) states that "the use of force involving cyber operations by a State in the exercise of its right to self-defense must be necessary and proportionate." This is consistent with what was stated in Article (52/2) of Additional Protocol I, which stipulated the concept of a military objective as "an object which by its nature, location, purpose or use makes an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage."

The third paragraph of the same article (52/3) confirmed that it is prohibited to target civilian objects if there is doubt as to whether they represent a military objective, as it states: "If there is doubt as to whether an object normally dedicated to civilian purposes, such as a place of worship, a house or other dwelling, or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used." This was confirmed by Rule (33) of the Tallinn Manual, which states: "In case of doubt as to whether an object normally dedicated to civilian purposes is being used to make an effective contribution to military action, the decision as to whether it is being used for such purposes should be taken after careful assessment of the situation." Likewise, in case of doubt as to whether a person is a civilian or a military person, Rule (33) came to interpret the doubt in favor of the civilian: "In case of doubt as to whether a person is a civilian or not, that person shall be considered a civilian."

The absence of an explicit provision in international law relating to cyber-attacks does not mean that the general rules relating to war stipulated in The Hague and Geneva Laws do not apply to these attacks. It must be understood that these general rules include developments regarding the means and methods of warfare, including the use of weapons, and the protection of vulnerable groups and civilian objects during armed conflicts. This was confirmed by Rule (20) of the Tallinn Manual, which states: "Cyber operations carried out in the context of armed conflict are subject to the law of armed conflict."

When these rules were adopted, they were designed in a way to include all developments related to armed conflicts, including technological and cyber developments. As a result, IHL can be considered applicable to cyber-attacks that form part of an armed conflict, when such attacks are linked to, and are part of, conventional means of warfare.

In addition, international humanitarian law can also be applied to cyber operations that rise to the level of armed conflict in terms of their effects, even in the absence of direct kinetic operations. This means that even if cyber-attacks do not involve conventional military activities, their effects could be considered sufficient to classify them as part of an armed conflict and therefore subject to the rules of international humanitarian law (Saud, 2018, pp. 90, 302).

The Tallinn Guide also defines a cyber-attack in accordance with international humanitarian law as an electronic operation, whether offensive or defensive, that is expected to cause injury or death to people or damage or destroy property. In addition, cyber-attacks can bring systems or devices down, causing physical damage. In other words, cyberattacks are both a means and a method of fighting (Al-Mousili, 2021, pp. 20-21).

In this context, viruses and worms can be considered like conventional weapons such as military devices and nuclear reactors, as they are used to carry out hacks or cyberattacks (El-Zahrani, 2017, p. 239). It is worth noting that in cases like these, the rules and principles of international humanitarian law can be applied to cyber-attacks, as they are considered part of cyber warfare.

An important point to focus on is estimating the impact of a cyber-attack, as it is considered a use of force if the impact of the attack compared to the actual use of force is equal to or close to it. In other words, if a cyber-attack has the same or similar effect as a conventional use of force, it can be considered a use of force under international humanitarian law. Also the International Committee of the Red Cross considers as stated in Article 69 of the Tallinn Guide that obstructing or disabling a particular system - whether an individual computer or a computer network - constitutes an attack under international rules relating to the conduct of hostilities. This type of attack is considered to be in violation of international humanitarian law regardless of the means used to carry

it out. This shows that the main crux lies in the actual effects of these attacks on the ground, rather than in the means used.

The uses of cyber operations during armed conflicts include many aspects, such as espionage operations, identifying targets, and influencing the enemy through psychological dimensions and information operations aimed at weakening his will and morale in battle. It also includes cutting off, disrupting, or misleading communications systems, and disabling radar stations and nuclear facilities. Cyber-attacks targeting civilian infrastructure, such as power plants, healthcare systems, humanitarian assistance programs and ambulance schemes, are extremely dangerous, especially for civilians. Examples of horrific cyberattacks include those currently occurring between Russia and Ukraine, which pose a major threat to global security and peace, posing a serious challenge to the international community and could spark a full-scale war.

It should be noted that international humanitarian law does not consider the use of force, whether kinetic or cyber, necessarily legitimate. In other words, no text included in international protocols or agreements such as the Geneva Conventions of 1949 can be considered to authorize or grant legitimacy to any act of aggression or use of force inconsistent with the Charter of the United Nations ((ICRC), 1949, p. Para. 2 of the preamble). This means that despite the existence of those international agreements and protocols that aim to regulate the behavior of warring parties and protect civilians and civilian facilities, they do not justify the use of violence or force in wars. In other words, even if there are laws regulating the behavior of warring parties, they do not permit the use of aggression or military escalation that contradicts the principles of the International Charter and the Charter of the United Nations, which aim to maintain international peace and security.

The damage caused by cyberattacks can be so devastating that they are equivalent to attacks armed with conventional military forces. For example, disruption of computer-controlled life support systems may result in death and injury to people at risk. A complete power outage can also disrupt vital community processes, leading to serious crises in vital sectors such as health and water. Moreover, the disruption of computers that control water plants and dams can lead to flooding in populated areas, resulting in massive human and material losses. These significant damages constitute strong evidence that cyberattacks

can rise to the level of an armed attack, with effects similar to those that conventional military force can have (Suleiman, 2020, p. 9).

This highlights the importance of studying and understanding cyber-threats comprehensively, taking the necessary measures to protect critical infrastructure and enhance cyber-security, and enhancing international cooperation to combat these attacks and reduce their impact on civilians and communities.

Based on the above, it is worth emphasizing that international humanitarian law does not legitimize the use of force, whether kinetic or cyber, if it conflicts with the UN Charter. Despite the existence of protocols and agreements such as the Geneva Conventions of 1949 that aim to regulate the behavior of warring parties and protect civilians, they do not justify aggression or military escalation. The damage caused by cyber-attacks can be devastating and equal to that caused by conventional military force, such as disrupting life support systems, power outages, or tampering with water stations and dams. These damages show that cyber-attacks may rise to the level of an armed attack in terms of impact, which calls for a comprehensive understanding of these threats and taking the necessary measures to protect vital infrastructure and enhance cyber security. Therefore, international responsibility must be activated to confront these threats, as cyber-attacks target the strategic interests of states and cause massive human and material losses, even without the use of conventional military force.

The researcher finds that the efforts to define a set of conditions that must be met for cyber-attacks to reach the level of an armed attack represent an important achievement, as they allow the attacked state to apply Article 51 of the UN Charter. However, these efforts can be criticized for being influenced by the traditional idea of the use of force as an equivalent to military force, and for relying on the stereotypical view of states about the concept of the use of force. We should take into account the continuous development of means of cyber-attacks and the changing goals of states at the present time, as states now consider these attacks as a means of superiority outside the scope of traditional military superiority, as is the case in the fields of communications, the financial market, the environment, nuclear plants, dams, and others.

As for the extension of the application of the rules of international humanitarian law to cyber operations that take place within an armed conflict, I will shed light on it in the second requirement.

2.2.2. Applying the principles of international humanitarian law to cyber attacks

The use of electronic warfare means follows the same principles that govern hostilities using conventional weapons, under international humanitarian law. IHL is flexible enough to keep pace with technological advances, showing diversity and flexibility in its application to various forms of weapons, including potential future methods and tactics. The International Court of Justice also emphasized the importance of adapting international humanitarian law to technological developments, by developing it in ways that make it applicable to all forms of weapons, including potential future methods and types. Accordingly, international humanitarian law is a mechanism for determining the limits of the use of means of electronic warfare during armed conflicts, just as it limits the use of any other weapons or means of warfare (Gisel et al., 2020).

In this context, Cordula Droege, Legal Advisor to the International Committee of the Red Cross, explained that the international humanitarian legal framework applies to cyber conflicts and must be respected. Claims that there are no laws in cyberspace and that international humanitarian law does not apply to cyber warfare have been denied, with experts pointing out that this situation is not unique, and the technology has witnessed previous developments and changes, and international humanitarian law and the laws of armed conflict have responded to these transformations in the past. Thus, it appears that the current legal framework is capable of dealing with these new developments without the need to establish cyberspace-specific legal rules (Gisel et al., 2020).

Article 4, paragraph 2, of the UN Charter addresses issues relating to the lawful use of force and war, prohibiting States from resorting to war or the threat or use of force against the territorial integrity or political independence of any State, unless this is consistent with the purposes of the United Nations. However, the Charter does not clearly define the meaning of "force" in this context, but rather leaves it to the Security Council to determine it depending on the circumstances surrounding each case. This is evident from Article 39 of the Charter which gives the Security Council the power to decide on coercive measures, meaning that Article 2, paragraph 4, of the Charter and related articles apply to cyber-

attacks regardless of the type of weapons used. Accordingly, this type of attack is considered a use of force within the meaning of Article 4, paragraph 2, of the Charter.

If a country is exposed to cyber operations, the UN Security Council must assess whether cyber-attacks constitute a threat to or violate international peace, or constitute a form of aggression (Al-Fatlawi, 2016, p. 49). The Council is therefore entitled to approve the adoption of non-coercive measures, including electronic operations, and if these measures are insufficient, it is entitled to issue a decision to adopt coercive measures, including electronic operations (Alwan, 2006, p. 34).

Any state has the right to respond to an armed attack resulting from activities on the Internet or a potential threat of such an attack using the right of self-defense provided for in Article 51 of the Charter, through electronic or traditional means. The United States did this in its 2011 International Cyberspace Strategy (Schmitt, 2017), pointing out that, under Article 51 of the Charter, there is no requirement to identify a specific kind of weapon in response to attacks. Instead, the response is drawn according to the physical impact of the attacks on the ground. As a result, a cyber-attack is deemed the use of force in light of its physical impacts and therefore constitutes a threat to international peace and security, and the attacked state is entitled to seek assistance from other states to deal with such attacks.

In this legal structure, there are certain rules and principles that are followed to safeguard those who are not directly involved in battles and to minimize the human suffering caused by armed forces. Thus, international humanitarian law is the legal regime that governs the conduct of parties to an armed conflict with a view to the protection of people affected by cyber-attacks and the enforcement of accountability, and the application of international humanitarian law proves its ability and desire to develop as new technologies emerge and the international context changes.

In the present scenario, international humanitarian law operates under certain guidelines so that the future development of electronic warfare and combat techniques is humane and respects human rights. From these principles, Article 36 is a part of Additional Protocol 1 that is annexed to the Four Geneva Conventions of 1949, which says that the contracting parties are required to ensure that any new development or use of weapons or weapons of war is compliant with the rules of international humanitarian law. Therefore,

any cyber-attacks are governed by the principles of international humanitarian law (Al-Mousili, 2021, p. 31), and the warring parties must follow the rules and restrictions that are set for them((ICRC), 1949, pp., Art. 53 of the First Additional Protocol). This principle is called the principle of limiting the right of parties to a conflict to choose military means and methods in order to avoid damage to civilians and civilian property.

But it is also important to note that international humanitarian law permits the parties to an armed conflict to take the necessary measures of defense, including how to deal with cyber-attacks, but this has to be done in a proportional manner and in accordance with the principles of international humanitarian law. This underlines the need to study the existing international laws and principles in relation to cyber conflicts and the proper use of the knowledge to protect civilians and minimize the devastating effects on them (El-Zahrani, 2017, p. 242).

Cyber-attacks can transform into an armed conflict even if the latter does not exist in the case of an attack on civilian life (El-Zahrani, 2017). For instance, when the cyber-attacks are directed at civilian persons or civilian objects, they have the same effects as conventional weapons; destruction, disruption of essential services, injuries, and possibly loss of lives. Due to the effect of cyber-attacks on civilians and civilian property, international humanitarian law rules and principles apply when it is used as a tool of warfare. According to these rules, the parties to the conflict have to protect human rights and minimize the catastrophic humanitarian impact of cyber operations. This is to safeguard the lives of people who should be protected, like the children, the sick, and other civilians who have no role to play in the conflict, as well as civilian property, which includes hospitals, schools, and other public facilities. This underlines the necessity to study the humanitarian effects of cyber-attacks and to apply the norms of the international humanitarian law regulating wars and conflicts to this sphere. Hence, the actualization of international humanitarian law is a useful mechanism in safeguarding the innocent populace and minimizing the adverse humanitarian effects of cyber-attacks.

By reviewing the Tallinn Manual, we find that the protection of children is included in the fourth section of the fifth chapter, specifically under Rule (78), which indicated that "it is prohibited to recruit or accept children as volunteers in the armed forces or to allow them to participate in cyber hostilities," which represents a true reflection of the content of the Fourth Geneva Convention for the Protection of Civilians (Articles: 23, 24, 50), as

well as Article (77) of the First Additional Protocol, and Article (4/3) of the Second Additional Protocol, annexed to the Geneva Conventions.

The Tallinn Manual included the protection of journalists in Section 5 of Chapter 5 (Rule 79), which states: "Civilian journalists engaged in dangerous professional missions in areas of armed conflict are civilians and must be respected as such, particularly with regard to cyber-attacks, as long as they do not take a direct part in hostilities." This represents a true reflection of the content of the protection of journalists against traditional military attacks, which is stipulated in Article (4/A) of the Third Geneva Convention, and Article (79) of the First Protocol of 1977.

The Tallinn Manual also included the protection of medical personnel and medical objects in the first section of Chapter Five (Rules: 70-73), which reflects what is stated in Articles (24-26) of the First Geneva Convention, Article (36) of the Second Geneva Convention, Article (20) of the Fourth Geneva Convention, and Article (15) of the First Additional Protocol.

The same can be done with reference to the principles of international humanitarian law as a basis for stating that cyber-attacks are regulated by this law. Of these principles, one of the most important is the principle of distinction between civilians and combatants; this is one of the fundamental principles of international humanitarian law. According to this principle, there is a difference between the people who do not take part in war and those who take part in military action or carry arms. This is where the "Martens Condition" comes in as an internationally accepted principle, Professor Fyodorovich Martens, the Russian delegate to the Hague Peace Conference in 1899, set this condition after the delegates at the peace conference failed to agree on the issue of the status of civilians who bear arms against the occupying forces, with the principle stating that in the absence of a specific rule in the recognized international law (Melzer & Kuster, 2017, p. 119), the civilians and combatants are subject to the protection and control of the principles of international humanitarian law and the principles of humanity as provided for in the customary law.

The principle of distinction between civilians and combatants has been incorporated in many international legal documents, the Preamble of the 1899 Hague Convention, for instance, in which it was stated that civilians should be protected and should not be

confused with persons involved in hostilities. This principle was also incorporated in the first Additional Protocol of 1977 and the Second Protocol of 1977, which clearly depicts that this principle is of immense significance in international law. Therefore, the "Martens Clause" and the principle of distinction between civilians and combatants are considered fundamental principles in determining the application of the rules of international humanitarian law to cyber-attacks, and they enhance the protection of civilians and limit the negative humanitarian consequences of these attacks. The International Court of Justice also confirmed in its advisory opinion on the legality of the threat or use of nuclear weapons, what is known as the "Martens Clause." This requirement is a recognized international legal principle that states that civilians and combatants are subject to the protection and authority of the principles of international humanitarian law as recognized by humanitarian principles and customary laws, in the absence of specific laws of international law.

In another context, the principles and rules of international humanitarian law apply to all forms of warfare and to all weapons, including future weapons whose use has not been prohibited or restricted by the international community. Although the principles of international humanitarian law were developed before the advent of nuclear weapons, there is no doubt that these principles apply to these deadly weapons and to new weapons technologies (Melzer & Kuster, 2017). It should be noted that there is no distinction between nuclear weapons and cyber-attacks with regard to the time of their circulation or their devastating effects (Al-Mousili, 2021, p. 32). Cyber-attacks may be more serious and destructive if they target nuclear plants on a large scale, which prompted the International Court of Justice to focus its opinion on the destructive nature of these weapons and on the harm resulting from their use on humanity, regardless of the means itself.

Therefore, international humanitarian law adopts principles and rules that apply to all forms of war and all weapons, including nuclear weapons and cyber-attacks, in order to provide protection for humanity and limit the negative humanitarian consequences of the use of these weapons.

This is not to mean that cyber-attacks are allowed by international humanitarian law since written rules concerning such are nonexistent, but rather they have to be judged by moral, humanitarian, and public conscience standards. These humanitarian principles are the

foundation of limiting military operations and safeguarding civilians and persons who do not take part in the conflict. Among these principles is the so-called "Martens Clause," which is regarded as the constituent part of the principles of the IHL. This condition is viewed as a suitable approach to address the rapid advancement in military technology, and it provides an opportunity to determine the prohibitions on the application of new military approaches and tools. Thus, the Martens Clause is of great significance in the sphere of application of international humanitarian law since it indicates the direction for further actions in relation to the challenges and problems occurring in connection with armed conflicts.

In general, IHL is believed to be capable of addressing new technologies and, therefore, cyber-methods. This means that through existing laws, humanitarian rules and principles can be applied to these developments without the need to create new rules for cyber space. As mentioned earlier, it is important to note that the principles of International Humanitarian Law are deemed to be principles of customary international law, which are fundamental and binding irrespective of the time, place, and circumstances (Saud, 2018, p. 91). Thus, they give the required legal advice and orientation to act in conditions of armed conflict, such as cyber-attacks, this is what was confirmed by Rule (21) of the Tallinn Manual, which states: "Cyber operations are subject to the geographical restrictions imposed by the relevant provisions of international law applicable during armed conflicts", without reference to new legal norms ((ICRC), 2022).

It is noteworthy that in the Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, the International Court of Justice did not directly point out that the principles of international humanitarian law apply to cyber-attacks, however, it implicitly did it taking into account that cyber-attacks are a new type of activity in the sphere of armed conflicts (El-Zahrani, 2017, p. 242). This is because of the need to understand the principles of international humanitarian law, which are cardinal to setting the parameters of military operations and safeguarding civilian persons and combatants. Despite the fact that cyber operations are viewed as a new type of conflict, the norms and standards of international humanitarian law can still be applied to them, taking into account the changing technical environment and new challenges that appear in the sphere of electronic warfare. The International Court reiterates that these principles are relevant to

any kind of war and any kinds of weapons existing at the time of the adoption of the treaty and future ones.

In this regard, the Court's opinion shows that humanitarian principles should be applied in the area of cyber-attacks in order to protect civilians and avoid possible human losses. This approach corresponds to the concept of international humanitarian law and its capacity to address new challenges in the sphere of electronic warfare and determines the course of actions that must be taken in order to maintain ethical standards and human rights in the context of new technologies.

Cyber-operations, in times of peace or in conditions of armed conflict, are governed by international humanitarian law, which sets out norms for their conduct and ways to prevent the adverse impact of cyber-operation on individuals and objects. International humanitarian law is the body of law that applies to all weapons and methods of warfare and offers more protection against the consequences of armed conflict. In this context, the principles of international humanitarian law regulating the conduct of hostilities, including cyber operations, apply. This comprises the principles of distinction, proportionality, and necessity, whereby the parties to the conflict have to differentiate between civilians and combatants as well as between military targets and civilian objects. It is important that all military actions be aimed at military targets and not at civilian targets ((ICRC), 1949, Art. 48 of the First Additional Protocol of 1977; Melzer & Kuster, 2017, pp. 77-98).

This principle applies to all military actions, including cyberspace operations that encompass the use of contemporary approaches and tools in warfare. Cyber-attacks are allowed only on military facilities and other objects that are both civilian and military during this use (Schmitt, 2013, Rule 39 of the Tallinn Manual). This aims to reduce civilian harm and protect civilian individuals from the effects of military conflicts, in line with the principles of international humanitarian law that seek to provide protection to all individuals affected by armed conflicts regardless of the form of weapons used or the nature of the attacks.

Parties involved in armed conflict must balance the need to use military force with humanitarian considerations. This balance aims to achieve military advantage with the least possible human and material losses ((ICRC), 1949, Art. 2/52 of the First Additional

Protocol of 1977). Force must be used in proportion to the desired objective of the conflict, which is to achieve the legitimate objective of the armed conflict such as victory over the enemy, while taking care to minimize human and resource losses. Thus, the destruction or seizure of enemy property is prohibited unless there is urgent military necessity. The principle of proportionality is that no attack should be undertaken that would cause loss of civilian life, injury or serious damage to civilian property, unless the military advantage gained significantly outweighs those losses. Furthermore, the Tallinn Manual prohibits cyberattacks that could result in significant loss of life or property, unless the military consequences of such attacks would significantly outweigh those losses (Saud, 2018, p. 94).

It is noted that targeted cyber-attacks on matters used for dual purposes pose a challenge to international humanitarian law. This challenge is due to the difficulty of distinguishing between the part of the electronic infrastructure that is used for military purposes and the part that is used for civilian purposes. Consequently, the whole target may turn into a military target and the civilian population may suffer when civilian infrastructure critical for the survival of the target is destroyed (Volkova, n. d.).

What has been identified is that the problem is not in the contrast between the uses of electronic structure and the different interactions of these uses. For instance, the specific electronic network that has been targeted may be used by the civilian population for business or to communicate, whereas the other end of the network may be employed by the military or intelligence services. This means that any attack on this infrastructure could lead to serious repercussions for the civilian population, as they are at risk of being indirectly harmed by attacks on electronic infrastructure important to their daily functions. This challenge entails strict compliance with the laws of armed conflict since the parties to the conflict bear the responsibility for the conduct of hostilities and the protection of civilians. Therefore, in order to safeguard civilians, belligerent parties need to implement strategies and measures that minimize the targeting of civilians and avoid the application of force that may produce unwanted outcomes for non-combatants.

International humanitarian law also provides special protection to civilian persons and civil assets in the context of armed conflict. The principles of international humanitarian law ensure that these vital structures are strongly protected against cyber-attacks. The use

of weapons and attacks targeting the civilian population indiscriminately are strictly prohibited, and disproportionate attacks that may cause unjustified harm are prohibited.

The Tallinn Manual also included special protection for the protected emblem, under Rules (62-65), and prohibited the improper use of protected emblems, symbols, banners, or signals mentioned in the law of armed conflict, as follows:

- Rule (62): Prohibition of the improper use of the United Nations emblem.
- Rule (63): Prohibition of the improper use of enemy emblems.
- Rule (64): Prohibition of the improper use of a neutral emblem.

In addition, international humanitarian law stresses the importance of respecting and protecting medical units and their personnel at all times. Therefore, cyber-attacks against these protected persons and structures are often considered a violation of international humanitarian laws. As for civilian data that does not enjoy special protection, such as tax data and bank records, international humanitarian law guarantees general protection of the civilian population from the effects of hostilities. Any exception to these data from the protection of international humanitarian law could open major gaps in the protection system established by international humanitarian law.

The researcher finds that the application of the principles of international humanitarian law to cyber-attacks, despite their importance, faces significant challenges. Despite the flexibility of international humanitarian law in adapting to technological developments, there is a large gap between theoretical legal texts and actual application on the ground. It is for this reason that the warring parties cannot be held fully accountable for cyber-attacks because of their highly technical nature and the fact that the perpetrators of the attack cannot be easily identified, thereby making it hard to uphold the principles of distinction, necessity, and proportionality.

On the other hand, it appears that the international community has not done enough to come up with a concrete and coherent legal regime for addressing cyber incidents. It may be disadvantageous to employ general principles of international humanitarian law, as these were developed for conventional warfare and may not be sufficient to address issues regarding cyber warfare. Technology is advancing at a very fast rate, and existing laws may not be able to check this development adequately.

Furthermore, the use of international humanitarian law in the context of the cyber domain needs robust international cooperation and genuine political will, which appear to be missing in many instances. Governments may be reluctant to limit their employment of potentially devastating cyber-attacks that can offer them immense tactical benefits.

Lastly, there is a need to reconsider how the principles of the IHL regulate cyber-attacks and potentially establish new protocols or agreements that would be adequate for the present and future challenges in the sphere of technology. There is a need for more differentiation on matters relating to attribution of blame, protection of non-combatants and their property, and compliance with humanitarian norms in cyber conflict.

Chapter Three
International Responsibility for Cyber Attacks

The notion of international responsibility is one of the most significant subject matters of international law in the contemporary world, particularly in view of the recent scientific advancements that have significantly influenced the relations between nations. These have given rise to new issues that were not covered by the conventional rules of international law, which required the handling of these issues in manners that are appropriate for them. Of these problems, cyber-attacks and the losses resulting from them are particularly noteworthy because the rules of international responsibility for them are still the subject of debate and controversy. Rule (6) of the Tallinn Manual referred to the legal responsibility of States, which states: "A State shall bear international legal responsibility for cyber operations attributable to it that constitute a breach of an international obligation." This further complicates the issue of defining how much these attacks are governed by the principles of international law and to what extent the damage that resulted from the attacks should be compensated. In this regard, it became essential to outline new and more progressive rules governing international responsibility, as well as to adjust these rules to modern challenges and guarantee justice in cyberspace. Improving the transparency and clarity of these rules helps to increase international security and stability and makes states accountable for their actions in all spheres, including the digital one, which corresponds to the development of international law and its adaptation to modern conditions. Accordingly, international responsibility for cyber-attacks will be addressed through the following three demands:

3. Definition of international responsibility

Some define international responsibility as: "the right of a person under international law to make good for the harm that he has caused, and to suffer the penalty as a punishment for this infringement, for the benefit of the victim (Al-Ghunaimi, 1993, p. 349).

The International Law Commission, in its 1957 draft, defined international responsibility as: "the attribution of an internationally wrongful act to a subject of public international law, which entails the obligation of that person to pay compensation or redress the damage resulting from this internationally wrongful act."

With this definition, the International Law Commission makes it clear that international responsibility is not merely an acknowledgment of the occurrence of a wrongful act but also includes practical obligations to redress the situation and compensate victims, reflecting the importance of maintaining international order and justice among States and other international entities (Abu Al-Wafa, 1990, pp. 45-47).

Some people think that international responsibility is "the process of attributing an act to a person subject to international law, whether or not this act is prohibited by international law, as long as it has caused harm to a person subject to international law, which calls for the imposition of a certain international penalty, whether this penalty is of a punitive nature or not" (Abu Aita, 2011, p. 250). In other words, international responsibility is a relationship between two persons subject to international law, where one of them is obligated to compensate for the harm he has caused to the other. Thus, it becomes clear that international responsibility is related to justice and correcting the situations resulting from acts that harm international relations, which enhances stability and security in the international system.

International jurisprudence and jurisprudence have helped to shape the rules of international responsibility in such a way as to respect international legitimacy, particularly in relation to the obligatory international norms that govern the fundamental and vital interests of humanity (Abu Aita, 2011).

International responsibility is understood as the legal regime that imposes an obligation on a state that has committed an act prohibited under international law to bear the costs of the harm inflicted on the attacked state. This definition helps to clarify that international responsibility is not only an admission of the fact of a violation but also the existence of practical measures for the elimination of harm and the restoration of the losses to the victims. International jurisprudence and jurisprudence work to strengthen this legal system by setting norms and principles that will enhance the delivery of justice in international relations and assist in maintaining global order and stability. Reparation for harm caused by acts that are unlawful under international law is equally important for this system because states are bound by responsibility for acts that result in the loss, thus creating confidence between states and encouraging cooperation at the international level within the framework of compliance with international law.

International responsibility in the old concept is limited in its scope and is based on three major principles. First, it applies only to persons of public international law, namely the state, which means that only states are accountable for their conduct in the international arena. Second, responsibility is limited to the civil aspect, where the state bears compensation as a means of repairing the damage caused by its actions. Third, the limits of responsibility stop at the damages inflicted on the state as a result of acts punishable by international law. This old concept of international responsibility reflects a limited scope of accountability, as it only includes states and deals with damages in a purely compensatory manner, without considering other dimensions that may require broader treatments. In this context, the main focus was on compensating the affected state for the losses it incurred due to the wrongful acts committed by another state, which reflects a legal system concerned with restoring the situation to what it was before the damage occurred and emphasizes the importance of compliance with international laws as a means of ensuring peace and stability between states.

In 2001, the International Law Commission defined international responsibility as "every internationally wrongful act of a State entailing its international responsibility." By this definition, any breach of international law committed by a state is grounds for assuming international responsibility. The International Court of Justice also stated that according to the principle of international law, a breach of an international obligation must be compensated by the violating state, and this obligation to compensate is an invariable corollary of any breach of any international agreement, irrespective of whether it has been expressly provided in the agreement or not. This explanation explains that international responsibility involves the state's duty to provide compensation for the harm it has committed and affirms that compensation is part of the international legal regime, as this principle strengthens respect for international laws and treaties and guarantees justice between States. These rules are eager to make States liable for their wrongful actions, thus making the international legal order more stable and increasing confidence between States.

In the Charouz Factory case, one of the most basic maxims of public international law was underlined, according to which, the breach of any rule of international law means that adequate reparation has to be paid to the injured party. This principle gives the notion that compensation is not just an incidental remedy but a principal and inherent corollary

of any breach of an international treaty (Al-Jundi, 1990, p. 4). This means that the international legal system pays much attention to the process of how the state that violated the rules has to be responsible for its action and has to offer a reparation that should restore the pre-violation situation or, in any case, compensate for the losses which the injured state or other subject of the international law has sustained. This obligation to compensate reinforces the idea that justice in international relations requires effective corrective measures to ensure that states comply with international laws and treaties. By emphasizing this principle, the international legal system enhances trust between states and encourages compliance with their international obligations, thus contributing to the maintenance of global peace and stability.

3.1. Elements of international responsibility for cyber-attacks

There is a great similarity between the domestic legal system and the international legal system. In the domestic legal system, the individual is the main person to whom the law imposes obligations and grants him rights. Similarly, in the international legal system, there are persons like states that bear legal responsibilities and possess legal capacities. Consequently, whenever a state does an act that produces an effect upon another state or several states, then that state incurs the burden of international responsibility for that act. These principles also apply to cyber-attacks committed by individuals under international law, leading to considerable harm. As such, cyber-attacks can be presumed to satisfy the criteria of international responsibility. However, the application of this responsibility poses significant challenges because there are no clear legal rules governing these attacks, as well as the inability to track the source of the attacks and, therefore, to identify the culprit with a high degree of accuracy. This vagueness creates difficulties in the implementation of the principles of international responsibility in the sphere of cyber space, which requires the emergence of more precise and clear legal norms in order to meet the challenges posed by modern technological advances and provide justice in this crucial area. Here we will explain the pillars of international responsibility for cyber-attacks, which are as follows:

3.1.1.The ratio of action to the state

International responsibility is not limited to the mere existence of a harmful or wrongful act, but rather this act must be linked to a fully sovereign, independent state. In the international legal system, the act must be attributed to a state that has full legislative,

executive, and judicial authority, in order to be held responsible for its own actions and the actions of its individuals or public officials. For example, member states of a federal state do not enjoy full sovereignty and cannot be held accountable in the same way as fully sovereign, independent states, because they are not subjects of public international law. Similarly, states that lack sovereignty or do not fully exercise their rights cannot be held accountable in the same way as fully sovereign states. This distinction reflects the importance of full sovereignty in determining the scope of international responsibility according to international law (Fouad, 2019, p. 277).

In the case of cyber-attacks, damage is inflicted as soon as these attacks are launched, targeting the country's critical infrastructure, which can result in significant damage. These attacks are usually carried out by advanced countries with significant cyber capabilities and may be carried out by multiple parties due to the ease of access to cyber infrastructure and the spread of international communications. The perpetrators of these attacks include nation states, governmental organizations, whether global or regional, in addition to specific individuals who have the ability to move freely in cyberspace, as well as terrorist groups, rebels, and national liberation movements. International responsibility in these cases requires proving the attribution of the act to the state, as states bear responsibility for the actions of their citizens if these actions violate international laws and cause damage to other states (Khalifa, 2015).

3.1.2. The act is internationally unlawful.

International jurisprudence has unanimously agreed that an unlawful act refers to acts that are considered to be in violation of the texts of international laws or general principles of law. This classification includes behaviors that are considered a violation of a state's international obligations, whether by committing a prohibited act or by refraining from an act that obliges it. The criterion of unlawfulness in international jurisprudence is considered an objective criterion, as the state bears legal responsibility for any violation of its international obligations, regardless of whether the source is local or international, which makes the classification of the act within the framework of international law without considering the internal details of the legal system or the means of committing the violation (Al-Taie, 2009).

In applying international laws to cyber-attacks, it becomes clear that these attacks are considered a violation of international law systems as they can cause significant material and human damage. This behavior contradicts the objectives of the United Nations, international humanitarian laws, and other rules of international law in general.

3.1.3. Harm

In the context of legal liability, damage is an essential element; if there is no damage, liability disappears. Damages can be classified into direct and indirect damages, depending on the damaged interest or the injured party. From the point of view of the aggressor, damage is divided into two types: material damage, which includes any material impact on the rights of an international legal person or its subjects, resulting in an apparent and tangible effect. The second type is moral damage: which is any infringement on the honor or reputation of an international person, or one of its subjects, i.e. moral damage is any attack on the right of international persons or their subjects, resulting in intangible effects (Abdel Khaleq, 2004, pp. 28-29).

When considering the impact of cyber-attacks, we find that harm is manifested in all its forms, regardless of whether the perpetrator is a nation-state, as in the case of the Iranian nuclear program, or a criminal organization seeking to inflict serious harm on others. These harms range from the theft of information to the hacking of bank accounts, to the theft of credit card numbers. Although the elements of international responsibility for cyber-attacks are available, identifying, monitoring, and tracking the perpetrators to bring them to justice is an extremely difficult task due to the anonymity of cyberspace. This major challenge complicates efforts to ensure justice and accountability and makes it difficult to protect digital infrastructure and individuals from the risks of ongoing attacks. The growth of cyber threats is increasing the speed at which technologies used in cyber-attacks are being developed, and thus, the identity of the attackers is hard to establish; therefore, there is a need to enhance international cooperation and monitoring and tracking systems to counter these threats.

3.2. Compensation

In order to properly discuss the concept of compensation for cyber-attacks it is necessary to define compensation in the legal context, its foundation in international humanitarian law, and the classification of compensation.

3.2.1. Meaning of compensation

The meaning of compensation as a legal term relates to the act of making good for a wrong or loss suffered by a person or an organization due to an unlawful act or mistake (Amer, 2020, p. 745).

3.2.2. Compensation in International Humanitarian Law

The general principles of the four Hague Conventions of 1907 contain rules that regulate legal norms of armed conflicts on the territory of states and require belligerents to follow specific standards during armed conflicts. These conventions are the foundation of international humanitarian law, which sets the standards of behavior during wars with the goal of safeguarding people and things. Where any of the belligerents infringe these provisions, he is required to make good the loss, if any in order to restore the victims or the injured parties. Furthermore, the belligerent remains fully liable for all actions performed by members of his armed forces, which expands the circle of responsibility not only to individual actions but to mass actions of forces subordinate to him ((UN), 2004, p. 73, Par. 152). This obligation to compensate reinforces the concept of accountability and emphasizes the need to bear legal and humanitarian responsibility for acts during armed conflicts, which contributes to achieving justice and reducing violations by providing a mechanism for holding those responsible to account and redressing the damages suffered by those affected.

The advisory opinion of the International Court of Justice on humanitarian law and human rights violations in the occupied Palestinian territories affirmed that Israel was under the legal duty to make reparation to all natural and juridical persons who have suffered direct loss or damage as a result of violations of humanitarian law and human rights. The Court further said that due to the construction of the wall and the regime that accompanied it, homes were seized, businesses and agricultural land were demolished, and major harm was inflicted on individuals and institutions. Therefore, the Court ruled that Israel should pay reparations to the individuals and entities affected and stated that such reparations encompass material, psychological, and moral compensation. This advisory opinion is an example of the international law principles that require accountability for wrongful conduct and adequate reparation for the injured. It is a measure within a series of actions to defend human rights and set legal responsibility for the actions that affect human life

and property, emphasizing the provision of international justice to bring justice and equity in numerous conflicts.

3.2.3. Forms of compensation for international liability

International responsibility has various legal consequences, but the most significant one is the responsibility of the state that has committed an unlawful act to make reparation for the harm caused. International courts have upheld this principle in many of their decisions, pointing out that compensation is not a one-size-fits-all concept. Of these forms, in-kind compensation seeks to bring things back to the state they were before unlawful conduct took place or at least to eliminate the military acts that have caused the loss. Non-monetary compensation is believed to be one of the most efficient ways of delivering justice as it aims to put things back to how they were as much as possible to restore fairness and justice to the affected parties. This is what the International Court of Justice confirmed that Israel has an obligation to immediately cease construction of the wall being built in the occupied Palestinian territories, and to remove the built-up parts inside the Palestinian territories, including East Jerusalem and the surrounding areas, without delay ((UN), 2004, p. 71, Para. 145).

Financial compensation for damage caused by a wrongful act may be provided. Financial compensation for damage caused by a wrongful act is the most common form of compensation in practice. The Permanent Court of Arbitration has indicated that financial compensation is an effective means of settling the various responsibilities of States, affirming that “there are no fundamental differences between the various responsibilities of States, and they can all be settled by the payment of a sum of money” (Abu Sakhila, 1981, p. 360). Often, the payment of damages is done under an out-of-court settlement whereby the parties involved sit down and negotiate on the amount and form of compensation that would be in proportion to the material and moral damages incurred by the injured. These negotiations are evidence of the parties’ desire to find a solution that would be fair to both parties and meet the common rights and interests, thus increasing the stability of international relations and promoting the peaceful settlement of disputes. Financial compensation is broad enough to include economic damage, psychological damage, and loss of life and property, which makes it a full way of compensating for damage and seeking justice.

Lastly, compensation can be in the form of an apology, which entails a state formally apologizing and expressing regret for the shortcomings of its soldiers or employees while in the execution of their duties. This form of compensation is crucial because it demonstrates that the state accepts the error and is willing to apologize for the wrongful actions that led to the loss (Abu Sakhila, 1981). They are delivered through diplomatic means, which assists in reducing tensions and restoring trust between the countries in disagreement or between the offending state and the aggrieved parties. Apology satisfaction improves the idea of restorative justice as compensation is not only confined to material losses, but it also deals with moral or psychological damage, which contributes to the overall aim of providing justice and healing the psychological harm that may have been done to the victims. In addition, a formal apology is a means of promoting international peace and security, as it sends a strong message about the state's commitment to international law and human rights and encourages the peaceful resolution of disputes and respect for the rights of the various parties.

The Tallinn Manual referred to the criminal responsibility of commanders and superiors, in Rule (24) thereof, which states: "A- Commanders and other superiors bear criminal responsibility for issuing orders for cyber operations that constitute war crimes. B- Commanders are also responsible if they knew or should have known, due to the circumstances prevailing at the time, that their subordinates were committing, about to commit, or had committed war crimes and (the commander) failed to take all reasonable and available measures to prevent the commission of such crimes or to punish those responsible," which is in line with the content of Article (25) of the Rome Statute of the International Criminal Court of 1998.

3.3. Legal responsibility for crimes of a cyber-nature in light of Palestinian legislation

Recent years have witnessed a significant increase in the use of cyberspace in all aspects of life, making it a new arena for conflict and competition between countries. Cyber-attacks are no longer just a threat to information and data but have become an effective tool used by countries to disrupt vital infrastructure, influence political and economic systems, and even destabilize countries.

The danger of cyber-attacks has increased with the development of the technologies used in them, as they have become more complex and advanced, and difficult to detect and track. Countries are now striving to enhance their defensive and offensive cyber capabilities, and develop national strategies for cyber security, with the aim of protecting their national interests from increasing cyber threats.

The Palestinian legislator has kept pace with this rapid technological and information development at the present time, which has become the basic feature of the current era, as many negative effects have resulted on the security and sovereignty of states, which prompted the Palestinian legislator to criminalize all acts that could constitute a threat to national interests, security and public order, which is what we find under the provisions and articles of Decision-Law No. (10) Of 2018 regarding cybercrimes, and its amendments.

As we review the articles of this decree-law, we find that Articles (39, 41, 42) include criminalizing everything that could constitute a threat to Palestinian national interests, whether these acts are committed from inside or outside Palestine:

Article (39/1) of the decision on the law on electronic crimes stipulates that "the competent investigation and control authorities, if they detect that websites hosted inside or outside the country are placing any phrases, numbers, pictures, films, or any promotional materials or other things that may threaten national security, public order, or public morals, shall submit a report on this to the Public Prosecutor or one of his assistants, and request permission to block the website or websites or block some of their links from display."

This legal text addresses the powers of the competent investigation and control authorities in confronting threats to national security, public order and public morals, which are published through websites hosted inside or outside the country. The text grants these authorities the authority to refer the matter to the Public Prosecutor or one of his assistants, and request permission to block the violating websites or their links. This text clarifies the scope of the powers of the investigation and control authorities, as it includes all websites that broadcast materials that threaten national security, public order or public morals, regardless of where they are hosted. It also specifies the types of materials that could pose a threat, including phrases, numbers, images, films, advertising materials, etc.

In addition to the procedures that investigation and control authorities must take in the event that they detect infringing materials, such that they must write a report on the incident and submit it to the Public Prosecutor or one of his assistants, and request permission to block the infringing site or its links ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 39).

The above text specifies the authority of the Attorney General or one of his assistants to take a decision regarding blocking the site or its links, so that he may grant permission to block if he is convinced that there is a real threat to national security, public order or public morals.

Accordingly, the entire text gives the investigation and control authorities broad powers to monitor content published on the Internet and take the necessary measures to protect national security, public order and public morals. However, it must be emphasized that it is important to ensure a balance between protecting these interests and protecting freedom of expression and human rights. The decision to block any website or its link must be based on clear and justified legal grounds and be subject to judicial oversight to ensure that this power is not exploited to suppress opposing opinions or violate personal freedoms.

The text refers to the importance of cooperation between investigation and control authorities and the Public Prosecutor in combating cybercrimes, and the measures taken to block websites must be proportionate to the nature of the threat posed by the published materials.

The researcher believes that this legal text is an important tool to confront cyber threats targeting national security, public order and public morals. However, it must be applied with caution and balance, while ensuring respect for human rights and fundamental freedoms.

Article (41) of the same Decree-Law referred to the duties of the state's agencies, institutions, bodies, and affiliated entities and companies, as the text of the article states the following: "The state's agencies, institutions, bodies, bodies, and affiliated companies are obligated to do the following:

1. Take the necessary preventive security measures to protect their information systems, websites, information networks, and their electronic data and information.
2. Expedite the notification of the competent authority of any crime stipulated in this Decree-Law, immediately upon discovering it or discovering any attempt to illegally intercept, intercept, or eavesdrop, and provide the competent authority with all information to uncover the truth.
3. Keep information technology data and subscriber information for a period of no less than (120) days and provide the competent authority with that data.
4. Cooperate with the competent authority to implement its powers."

The legal text includes a set of important obligations that fall on the shoulders of state agencies, institutions, bodies, entities and affiliated companies, in the field of cyber security. These obligations aim to protect the information systems, data and electronic information of these entities, and to ensure their cooperation with the competent authorities in combating cybercrimes.

The main obligations of international bodies are as follows:

First: Taking preventive security measures: The legal text requires the relevant authorities to take all necessary security measures to protect their information systems, websites, information networks, data and electronic information. This includes implementing strict security policies, using advanced protection technologies, training employees on the basics of cyber security, and conducting periodic tests to detect vulnerabilities ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 41/1).

Second: Immediate reporting of cybercrimes: The legal text requires the concerned parties to quickly report to the competent authority any crime stipulated in the law, immediately upon discovering it or discovering any attempt to illegally capture, intercept or eavesdrop. It also requires them to provide the competent authority with all the information necessary to uncover the truth. This obligation aims to ensure a rapid

response to cybercrimes, prevent the escalation of their damage, and prosecute their perpetrators ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 41/2).

Third: Retention of IT data: The legal text requires the relevant authorities to retain IT data and subscriber information for a period of no less than 120 days, and to provide the competent authority with that data upon request. This commitment helps in investigating cybercrimes, tracking down their perpetrators, and bringing them to justice ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 41/3).

Fourth: Cooperation with the competent authority: The legal text emphasizes the necessity of the concerned authorities' cooperation with the competent authority to implement its powers in the field of cyber security. This cooperation includes providing all necessary facilities, supplying them with the required information and documents, and complying with its directives. This commitment aims to ensure the effectiveness of efforts made to combat cybercrimes and protect the cyber security of the state and its institutions ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 41/4).

The importance of the legal text that we analyzed lies in the fact that it is considered an important step towards enhancing cyber security in the country and protecting its interests and the interests of its institutions from increasing cyber threats. By defining clear and specific obligations on the relevant parties, this text contributes to raising awareness of the importance of cyber security and improving the ability to effectively confront cybercrimes.

In addition, the aforementioned legal text represents part of an integrated cyber security system that seeks to protect the state and its institutions from cyber threats. By adhering to the provisions of this text and cooperating with the competent authorities, the concerned parties can effectively contribute to enhancing cyber security and protecting national interests.

The Palestinian legislator did not neglect the strategies of international cooperation with other countries in order to confront and combat cybersecurity crimes that threaten the interests, security and public order of the state, which was confirmed by Article (42) of the Decree-Law of 2018 regarding cybercrimes, which stipulated: "1. The competent authorities shall facilitate cooperation with their counterparts in foreign countries within the framework of ratified international, regional and bilateral agreements, or apply the

principle of reciprocity, with the aim of accelerating the exchange of information, which would ensure early warning of information and communication system crimes, avoid their commission, assist in investigating them, and track down their perpetrators. The cooperation referred to in the previous paragraph depends on the commitment of the foreign country concerned to maintain the confidentiality of the information referred to it, and its commitment not to refer it to another party or exploit it for purposes other than combating the crimes specified in this Decree-Law" ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 42).

The legal text addresses the issue of international cooperation in the field of combating information and communication system crimes and defines the legal and procedural framework for this cooperation. This analysis aims to gain a deeper understanding of the content of the text and its importance in strengthening international efforts to combat these crimes:

Paragraph 1 of Article 42: Facilitation of international cooperation

The first paragraph emphasizes the importance of international cooperation in the field of combating information and communication system crimes. It obliges the competent authorities to facilitate this cooperation with their counterparts in foreign countries, through:

International, regional and bilateral agreements: These agreements are the legal framework governing international cooperation in this field and define the mechanisms for exchanging information and providing legal assistance. The principle of reciprocity: In the absence of agreements, the competent authorities may cooperate with foreign countries on the basis of the principle of reciprocity, i.e. providing assistance on condition that the foreign country provides the same assistance in return. Expediting the exchange of information: Information must be exchanged quickly and effectively, so that early warning of information and communication system crimes can be provided, their commission can be prevented, investigations can be assisted, and perpetrators can be tracked ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 42/1).

Paragraph 2 of Article 42: Conditions of international cooperation.

The second paragraph sets two basic conditions for international cooperation in the field of combating information and communication system crimes, which are: Maintaining the confidentiality of information: The foreign state receiving the information must maintain its confidentiality and not disclose it to any other party. Not exploiting the information for other purposes: The foreign state must not exploit the information transferred to it for any purpose other than combating the crimes specified in this decision-law.

This legal text is of great importance in enhancing international cooperation in the field of combating information and communication system crimes, through: Defining the legal framework for cooperation: The text provides a clear legal framework for international cooperation in this field, which facilitates the exchange of information and the provision of legal assistance. Defining the conditions for cooperation: The text sets clear conditions for cooperation, ensuring the protection of the confidentiality of information and preventing its exploitation for other purposes. Encouraging international cooperation: The text encourages countries to cooperate in the field of combating information and communication system crimes, which increases the effectiveness of international efforts in this field ("Law by Decree No. 10 of 2018 on Cybercrime," 2018, Art. 42/2).

Accordingly, this legal text is considered an important step towards enhancing international cooperation in the field of combating information and communication system crimes. By facilitating cooperation and defining its conditions, this text contributes to protecting the security of states and the international community from these increasing crimes.

Conclusion

After reviewing the concept of cyber-attacks within the framework of contemporary international organization, it becomes clear that these attacks occupy a prominent position in specialized legal studies compared to other international issues that threaten international peace and security. Cyberspace has become a new arena for conflict between states, where cyber-attacks are used as a decisive means of controlling states by targeting both military and civilian infrastructure. These attacks result in severe cross-border effects that may amount to threatening international peace and security. Hence, the issue of adapting these attacks in the absence of a special international agreement regulating them strongly emerges. Through this study, a set of results and recommendations were reached that we believe are necessary to strengthen the legal system that frames cyber-attacks committed by one state against another, whether in times of peace or during war.

Results

1. The concept of cyber is still not internationally agreed upon, which calls for intensified international efforts to clarify and define it clearly. This is essential for any international agreement that may regulate the use of cyberspace in the future.
2. Cyber warfare represents a natural evolution in the concept of warfare, as it has moved it to a new generation based on remote control and domination. These wars have had a devastating global impact, as they can lead to the destruction of a country's infrastructure, including its water dams, nuclear reactors, and vital centers.
3. Cyber warfare is very attractive compared to its traditional counterparts due to its low cost. This attractiveness drives countries and groups to launch cyber attacks using advanced electronic weapons and specialized human skills. What distinguishes these attacks is that they can be carried out at any time, whether in peacetime, wartime, or crises. Moreover, these attacks do not take much time to perform and can be performed by groups that do not possess great power or capability, which makes cyber warfare a convenient and efficient weapon for achieving military and political objectives with less power and more efficiency.

Recommendations

1. The need to update both defensive and offensive capabilities is rooted in the increasing threat of cyber warfare. Hence, countries need to strive to modernize their

defense activities to address these risks through significant investment in and protection of information infrastructure. This includes modernizing military capabilities and increasing the level of readiness for such wars through regular training as well as through international cooperation in the protection of critical information infrastructure. Furthermore, efforts are invested in enhancing the effectiveness of human capital within the appropriate national bodies.

2. Strengthening the rules of international humanitarian law through the conclusion of international agreements to address crimes related to cyber wars and regulate all stages of such wars. This development calls for flexibility of the legal rules in order to capture the specificity of cyber-attacks which can cause destruction beyond that of traditional wars at the global level. Cyber wars are unique in their nature as they can shut down all the critical sectors of global society in the blink of an eye and at the same pace, which is why they should be tightly regulated through legal measures.
3. Applying international humanitarian law to cyber-attacks seeks to eliminate the possibility of a disaster that is beyond national territories and affects the world's important infrastructure. To this end, there must be provisions in international treaties that are particularly focused on the issue of these attacks and the ways to monitor and address them. It also improves the capacity of international humanitarian law to effectively undertake its main task of preventing the civilian population and infrastructure from suffering severe consequences of cyber wars.
4. By adopting such agreements, the international community can enhance cooperation and coordination to confront cyber threats more efficiently, by agreeing between countries to develop a comprehensive international agreement that addresses the use of cyber weapons, in line with the regulation of nuclear, chemical, biological and other advanced weapons. Cyberspace is considered a new arena for conflicts, and cyber weapons have enormous destructive potential that can threaten the vital infrastructure of countries and destabilize international security and stability. Therefore, reaching a comprehensive international agreement will establish a clear legal framework that defines how these weapons are used and sets strict controls to prevent their random or hostile use.

Through this agreement, mechanisms can be put in place to monitor, inspect and ensure that countries adhere to agreed laws, which enhances trust between countries and reduces

the likelihood of cyber conflicts. In addition, this agreement will contribute to enhancing international cooperation in the field of cyber security and the exchange of information and expertise to confront cyber threats more effectively. Concluding such an international agreement will protect sensitive infrastructure and ensure the use of cyberspace in peaceful and safe ways, which contributes to maintaining international peace and security.

References

(ICJ), I. C. o. J. (1986). *Military and Paramilitary Activities in and Against Nicaragua (Nicaragua V. United States of America): Merits*. International Court of Justice.

(ICJ), I. C. o. J. (1998). *Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, Summary of Judgments and Advisory Opinions of the International Court of Justice 1992-1996,* . United Nations Publications.

First Additional Protocol of 1977 annexed to the Geneva Conventions of 1949, (1949).

(ICRC), I. C. o. t. R. C. (2022). Cyberspace is not a legal vacuum, including during armed conflict. *International Committee of the Red Cross (ICRC)*. https://www.icrc.org/en/document/cyberspace-not-legal-vacuum-including-during-armed-conflict

(UN), U. N. (2004). *ICJ Advisory opinion on the Legal Consequences of the Construction of a Wall in the OPT*

Abdel Khaleq, H. (2004). *Responsibility and Punishment for War Crimes with a Study of its Application to War Crimes in Bosnia and Herzegovina*. Dar Al-Jamia Al-Jadida for Publishing.

Abu Aita, E. (2011). *International Sanctions between Theory and Practice* University Culture Foundation.

Abu Al-Wafa, A. (1990). Conditions of International Responsibility. *Diplomatic Magazine*(13), 45-47.

Abu Sakhila, M. A. a.-A. (1981). *International Responsibility for Implementing United Nations Resolutions*. Dal El-Marefa.

Al-Basha, F. Y. (2001). *Organized Crime under International Agreements and National Laws* (1st ed.). Dar Al-Nahda Al-Arabiya.

Al-Dulaimi, H. (2018). *Technological Development and Its Impact on States Sovereignty* University of Anbar]. Iraq

Al-Fatlawi, A. D. A. O. (2016). Cyber attacks: its concept and arising international responsibility In the light of contemporary international organization. *AL-Mouhaqiq Al-Hilly Journal for legal and political science*, *8*(4), 610-687.

Al-Ghunaimi, M. T. (1993). *The Mediator in the Law of Peace*. Mansha'at Al-Ma'arif.

Al-Hamdan, M. F. (2016, 02/02/2016). The position of international law on cyber warfare *Al-Riyadh* https://www.alriyadh.com/1124892

Al-Jundi, G. (1990). *International Responsibility* (1st ed.). Al-Tawfiq Press.

Al-Mousili, N. A. (2021). *Cyber-Attacks in Light of International Humanitarian Law* Syrian Virtual University].

Al-Taie, S. (2009). *The Right of Recovery in International Law*. Modern University Library.

Aleisaa, T., & Enab, O. (2019). International Responsibility for Cyber-Attacks in Light of the Contemporary International Law. *Zarqa Journal for Research & Studies in Humanities*, *19*(1).

Alsaade, N. (2022). Cyber war in light of the provisions of public international law. *Legal Research Journal*, *7*(2), 1-30.

Alwan, A. K. (2006). *The Mediator in Public International Law*. House of Culture.

Amer, S. E.-D. (2020). *Introduction to the Study of Public International Law*. Dar Alnahda.

Applegate, S. (2015). Cyber conflict: Disruption and exploitation in the digital age. In *Current and emerging trends in cyber operations: policy, strategy and practice* (pp. 19-36). Springer.

Bayoumi, A. R. (2012). *The Dangers of Israeli Weapons of Mass Destruction on Arab National Security,* (9th ed.). Dar Al Nahda Al Arabiya.

Cheraitia, S. (2020). Cyber sovereignty in China between the requirements of power and the

imperatives of national Security. *Algerian Review of Security and Developement*, *9*(1), 396-410.

Convention on Cybercrime, (2001).

El-Zahrani, Y. (2017). Strategic and Legal Dimensions of Cyber War. *The Research and Studies*, *14*(1), 225-248.

Elagab, O. (1986). *The legality of non-forcible counter-measures in international law* University of Oxford].

Fouad, M. A. (2019). *International Humanitarian Law*. University Publications House.

Gabčíkovo-Nagymaros Project (Hungary/Slovakia), ICJ (International Court of Justice (ICJ) 1997).

Gervais, M. (2012). Cyber attacks and the laws of war. *Journal of Law & Cyber Warfare*, *1*(1), 8-98.

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International review of the Red Cross*, *102*(913), 287-334.

Hathaway, O. A., Crootof, R., Levitz, P., & Nix, H. (2012). The law of cyber-attack. *Calif. L. Rev.*, *100*, 817.

Hughes, R. (2010). A treaty for cyberspace. *International Affairs*, *86*(2), 523-541.

Khalifa, I. A. H. (2015). Cyberspace and the Threat to Egyptian National Security, . *Arab Center for Cyberspace Research*.

Law by Decree No. 10 of 2018 on Cybercrime, (2018).

Lin, H. (2012). Cyber conflict and international humanitarian law. *International review of the Red Cross*, *94*(886), 515-531.

Melzer, N., & Kuster, E. (2017). International humanitarian law. *General course. Committee of the International Red Cross. M*, 184.

Nacib, N. (2021). Cyber War from the Perspective of International Humanitarian Law. *Critical Journal of Law and Political Science*, *16*(4), 218-236.

Samoudi, R. (2018). The Right to Self-Defense in Response to Cyber-Attacks in Light of International Law. *University of Sharjah (UoS) Journal of Law Sciences*, *15*(2), 336-362.

Saud, Y. (2018). Cyber Warfare in Light of the Rules of International Humanitarian Law. *The Legal Journal*, *4*(4), 80-108.

Schmitt, M. (2017). Computer network attack and the use of force in international law: thoughts on a normative framework. In *The Use of Force in International Law* (pp. 379-431). Routledge.

Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in bello. *International review of the Red Cross*, *84*(846), 365-399.

Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare* (A. M. K. Al-Moussawi, Trans.). Cambridge University Press.

Shafiq, N. (2016). *The Impact of Cyber Threats on International Relations: A Study in the Dimensions of Cyber Security*. Arab Bureau of Knowledge.

Shin, B. (2011). The Cyber Warfare and the Right of Self –Defense: Legal Perspectives and the Case of the United States. *IFANS*, *19*.

Smith, T. W. (2002). The new law of war: Legitimizing hi-tech and infrastructural violence. *International Studies Quarterly*, *46*(3), 355-374.

Suleiman, A. F. A. (2020). The Right of Legal Defense against Cyber Attacks. *Tikrit University Journal of Law*, *4*(4).

Toure, H. I. (2011). The International Response to Cyberwar. *The Quest for Cyber Peace*, 86-103.

United Nations Charter. (1945). https://www.un.org/en/about-us/un-charter/full-text

Verri, P., Croix-Rouge, C. i. d. l., Mottier, I., & Bouvier, A. A. (1988). *Dictionnaire du droit international des conflits armés*. Comité international de la Croix-Rouge.

Volkova, E. (n. d.). Protection des infrastructures de santé contre les cyberattaques dans les conflits armés. https://www.calameo.com/books/006401546497064e46e94

جامعة النجاح الوطنية
كلية الدراسات العليا

المسؤولية القانونية عن الحروب السيبرانية في ضوء قواعد وأحكام القانون الدولي اللإنساني

إعداد
نادية جواد توفيق زيد الكيلاني

إشراف
د. محمد حسين محمد ابو الرب

قدمت هذه الاطروحة استكمالا لمتطلبات الحصول على درجة الماجستير في القانون الدولي وحقوق الإنسان
بكلية الدراسات العليا في جامعة النجاح الوطنية، نابلس، فلسطين.
2025

المسؤولية القانونية عن الحروب السيبرانية في ضوء قواعد وأحكام القانون الدولي اللإنساني

إعداد

نادية جواد توفيق زيد الكيلاني

إشراف

د. محمد حسين محمد ابو الرب

الملخص

تتناول هذه الدراسة المسؤولية القانونية عن الحرب السيبرانية في ضوء قواعد وأحكام القانون الدولي الإنساني. وتبحث في كيفية تطبيق القانون الدولي الإنساني على الحروب السيبرانية، مسلطة الضوء على التحديات الفريدة التي تُشكِّلها التطورات التكنولوجية الحديثة، وضرورة تكييف الأطر القانونية القائمة لمواجهتها بفعالية.

تكمن أهمية هذه الدراسة في تركيزها على تعريف مفهوم الحرب السيبرانية وتقييم مدى انطباق مبادئ القانون الدولي الإنساني في تنظيم الهجمات السيبرانية أثناء النزاعات المسلحة. فعلى الرغم من إرساء مبادئ القانون الدولي الإنساني التأسيسية من خلال اتفاقيات جنيف الأربع لعام 1949 والبروتوكولين الإضافيين لعام 1977، فإن التطور السريع للتكنولوجيا يستلزم إعادة النظر في هذه القوانين في سياق الحرب السيبرانية.

تتمحور مشكلة البحث حول غياب نهج قانوني وإنساني متكامل للحرب السيبرانية، مبرزة صعوبة مقارنة الحرب التقليدية والحرب السيبرانية. تعتمد الدراسة منهجية تحليلية، تدرس تطبيق مبادئ القانون الدولي الإنساني على أنشطة الفضاء السيبراني التي تقوم بها الجهات الفاعلة الحكومية وغير الحكومية في الحالات التي تُصنّف على أنها نزاعات مسلحة. تنقسم الدراسة إلى ثلاثة فصول رئيسية:

يستكشف الفصل الأول طبيعة الحرب السيبرانية وأصلها، وتعريفها، وتصنيفها ضمن الأطر القانونية القائمة.

يبحث الفصل الثاني في كيفية انخراط الجهات الفاعلة الحكومية وغير الحكومية في الحرب السيبرانية، وأهدافها، وتداعياتها على الاتفاقيات الدولية والقواعد العرفية للنزاعات المسلحة.

يركز الفصل الثالث على الاعتبارات القانونية والأخلاقية للحرب السيبرانية، ويحلل كيفية تطبيق مبادئ مثل التناسب والتمييز وحماية المدنيين على العمليات السيبرانية.

تختتم الدراسة بمجموعة من النتائج والتوصيات، مؤكدةً على أهمية تحديث القانون الدولي الإنساني وتوسيع نطاقه لمواكبة الطبيعة المتطورة للحرب. من أهم النتائج الحاجة الملحة لتوضيح التصنيف القانوني للحرب السيبرانية، وضرورة التعاون الدولي في وضع أطر للدفاع والأمن السيبرانيين. تدعو التوصيات الرئيسية إلى تعزيز التعاون بين الدول والمنظمات الدولية لوضع تدابير عملية وقابلة للتنفيذ لتنظيم مخاطر الحرب السيبرانية والتخفيف منها.

الكلمات المفتاحية: المسؤولية القانونية، الحروب السيبرانية، قواعد وأحكام القانون الدولي اللإنساني.