Remittances Review
August 2024,
Volume: 9, No: 4, pp.2424-2438
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)

Received: 04 July 2024, Accepted: 10 August 2024
DOI: https://doi.org/10.33282/rr.vx9i2.132

Legal regulation of international cyber conflicts

Laid Rai[1], Salem Haoua[2], Abdlhakim Moulay Brahim[3].

[1,2,3] University of Ghardaia (Algeria).

The Author's Email: rai.laid@univ-ghardaia.dz[1], haoua.salem@univ-ghardaia.dz[2], moulaybrahim.abdlhakim@univ-ghardaia.dz[3]

Abstract:

The proliferation of cyber capabilities has fundamentally transformed the nature of armed conflicts in the 21 st century, presenting unprecedented challenges to international humanitarian law as the legal regime regulating modern armed conflicts.

This paper explores the difficulties and the prospects surrounding the international regulation of cyber warfare, by examining both the existing legal frameworks and the emerging norms and practices in this evolving domain.

Keywords: The international humanitarian law; armed conflicts; regulation; cyber warfare.

Introduction

War has always shaped the diaries of humans and their history, as scarcely a time or place is devoid of the outbreak of wars and acts of violence, the results of which are the death of individuals and the destruction of property. Despite this reality, which has become self-evident, it is impossible, indeed futile, to conceive the possibility of eliminating the phenomenon of war or resorting to the use of force. It is true that the international legal system criminalizes resorting to war in international relations[1], and limits the cases in which states are permitted to resort to the use of force to cases of legitimate defense[2], the enforcement of sanctions decided by the Security Council under Chapter VII of the United Nations Charter[3]. Despite this qualitative development, humanity continues to suffer from war, even if they are legitimate. Therefore, the path of prohibiting war must be paralleled by a path of alleviating the suffering of humans during and after wars.

Remittances Review
August 2024,
Volume: 9, No: 4, pp.2424-2438
ISSN: 2059-6588(Print) | ISSN 2059-6596(Online)

The reality of armed conflicts, with the invention of deadly weapons and the innovation of new combat methods for instance cyber warfare, has led to the need for adapting more effective protection under international humanitarian law through the formulation of new conventions and protocols.

The problem addressed in this research paper revolves around 'the extent to which international legal regulation of electronic armed conflicts is possible?

THE FIRST TOPIC INTERNATIONAL LEGAL REGULATION OF ARMED CONFLICTS

Even the use of force in international relations is prohibited by the United Nations Charter reaffirmed this rule, as Article 4, paragraph 2 which emphasizes that member states shall refrain from the use of force in their relations with other states. The international humanitarian law through the Hague law and Geneva law regulates armed conflicts.It encompasses a set of rules to limit the effect military operations and mitigate human suffering.

First requirement: International humanitarian law regulates armed conflicts

The international humanitarian law regulates modern armed conflicts in either methods and means of warfare which minimize the number of casualties among fighters, afford protection to non – fighters, civilians and civilian assets.

First section: The emergence of international humanitarian law

The emergence of international humanitarian law is the fruit of the crystallization of the conviction that the most important shared values between all civilizations are, firstly, the reconciliation between the necessities of war and humanitarian considerations, and secondly, the vital importance of respecting the human person and the most basic humanitarian considerations. The embodiment of these noble ideas has required a path that traces its beginnings to the end of the nineteenth century and continues in the present, extending into the future. Fighters have always been subject to local rules and customs that regulate the conduct of warfare, the source of these rules may be religious or the will of a governing authority.

The Battle of Solferino, with its thousands of casualties and wounded, prompted Henry Dunant to contemplate mechanisms to alleviate the horrors of war. Dunant envisioned the establishment of an organization to provide assistance, leading to the creation of the International Committee of the Red Cross, which became a symbol of implementing international humanitarian law. The committee's success in fulfilling its mandate lies in its neutrality and objectivity, earning respect from all countries.

The first attempt in modern times to regulate the rules of war dates back to the regulation drafted by François Lieber, a law professor at Columbia

University in New York. The rules contained in this regulation became effective after the President of the United States ratified it, binding the federal forces involved in the Civil War between the North and the South from 1861 to 1865. In 1864.

The first international treaty on the laws and customs of war to protect military casualties was drafted, known as the Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. This convention laid the foundation for what became known as the Geneva Conventions, which aimed protecting non-combatants such as civilians and medical personnel. These agreements were amended for the first time in 1906 and 1929, then again in 1949 after World War II. Conversely, peace conferences held in The Hague between 1899 and 1907 provided an opportunity to establish a system known as the Hague Law through the drafting of conventions regulating the methods and means of warfare.

second section: Definition of international humanitarian law

The international humanitarian law, also known as the law of armed conflict, is defined as an important branch of general international law that owes its existence to a sense of humanity. It focuses on protecting individuals in war, aiming to safeguard those affected by armed conflicts from suffering and to protect civilian assets not directly related to military operations.

International humanitarian law is defined as a treaty-based legal system based on a set of treaty texts that precisely define rules related to either methods and means of warfare or the protection of specific categories .

second requirement: Legal regime of international humanitarian law

Armed conflicts are regulated through the Hague law and Geneva law. in either methods and means of warfare in order to minimize the number of casualties among fighters, and to protect non – fighters, civilians.

First section: International humanitarian law conventions

International humanitarian law is composed of a set of treaties and protocols that defines rules related to either methods and means of warfare or the protection of specific categories. These texts include the following:

- The Hague Convention II of 1899 regarding the rules and customs of land warfare.
- The Hague Convention VI of 1907 regarding the rules and customs of land warfare.

- Geneva Convention I of 1949 concerning the improvement of the condition of wounded and sick members of the armed forces in the field, amended by the conventions of 1864 and 1906.
- Geneva Convention II of 1949 concerning the improvement of the condition of wounded, sick, and shipwrecked members of the armed forces at sea, amended once.
- Geneva Convention III of 1949 concerning the treatment of prisoners of war, amended from the convention of 1929.
- Geneva Convention IV of 1949 concerning the protection of civilians during wartime.
- The First Protocol of 1977 relating to the protection of victims of international armed conflicts.
- The Second Protocol of 1977 relating to the protection of victims of non-international armed conflicts.

The Geneva Conventions have acquired customary status, meaning that all parties and even non-parties are bound by the obligations they entail. The Court based its determination on the following argument: the majority of the world's countries have acceded to these conventions, indicating broad acceptance. The International Court of Justice affirmed in the "Corfu Channel" case of 1949 that Albania was obligated to warn of the presence of mines because the 1907 Convention is binding on all states, even those not party to it. Albania's failure to fulfill this obligation constituted a violation of the customary rule of ensuring peaceful navigation. The Court reiterated its previous opinions in the "Nicaragua" case of 1986. It confirmed the customary nature of the rules contained in the regulations annexed to the Hague Convention VI of 1907, which the Nuremberg Military Tribunal adopted as an interpretation of the laws of war and their customs. The International Court of Justice went further in its advisory opinion on reservations to the Genocide Convention issued in 1951 by endowing the prohibition of genocide with the status of a peremptory norm[4]. The Court relied on two criteria in its determination: first, the primary purpose of the Convention is to achieve humanitarian and civilizational objectives distinctly, and second, there is no special interest for states but rather a common interest for all. Subsequently, the International Court of Justice affirmed in the "Barcelona Traction" case of 1970 that the obligation to prohibit the crime of genocide, borne by the parties to the Convention, rises to the level of an obligation erga omnes, and it reaffirmed this in the "Application of the Convention on the Prevention and Punishment of the Crime of Genocide" case of 1996.

The evolution of armed conflicts, with the invention of deadly weapons and the innovation of new combat methods, has led to the need for adapting protection under international humanitarian law through the formulation of new conventions and protocols:

- The Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict of 1954.
- The Convention on the Prohibition of the Development, Production, and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on Their Destruction of 1972.
- The Convention on Certain Conventional Weapons That May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects.
- The Chemical Weapons Convention of 1993, which prohibits the development, production, stockpiling, and use of chemical weapons.
- The Protocol on the Prohibition of the Use of Chemical Weapons, the Chemical Weapons Convention, and on Their Destruction of 1995.
- The Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on Their Destruction of 1997.
- The Rome Statute of the International Criminal Court of 1998.
- The Protocol to the Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict of 1954.
- The Optional Protocol to the Convention on the Rights of the Child on the involvement of children in armed conflict.

These conventions and protocols aim to provide enhanced protection for civilians, cultural heritage, and the environment during armed conflicts, as well as to regulate the use of specific types of weapons.

.second section: International Humanitarian Law Rules

The conduct of hostile operations necessitates the establishment of a set of principles that define the nature of weapons and methods for conducting military operations:

- Principle of Distinction Between Combatants and Non-Combatants: This principle is the cornerstone of international humanitarian law as it restricts hostile operations to combatants, thus enabling the protection of civilians[5]. Its essence lies in the absolute prohibition of deliberate attacks against civilians and the use of indiscriminate weapons, as civilians are the ones most affected by them.

- Principle Prohibiting the Use of Weapons Causing Unnecessary Suffering or Injury[6].The International Court of Justice, in its advisory opinion on the threat or use of nuclear weapons in 1996, defined the concept of unnecessary suffering for combatants as harm exceeding that which cannot be avoided to achieve legitimate military objectives. The Court emphasized that the criterion for determining this is the balance between the degree of injury and the military advantage sought, requiring an assessment of each case individually.
- Martens Clause[7]: The Martens Clause stipulates that civilians and combatants remain under the protection and authority of the principles of international law as derived from customary law, humanitarian principles, and the dictates of public conscience, even in situations not covered by specific treaties or other international agreements[8]. Some consider the Martens Clause to be a mere verbal evasion because its content is debated between two factions. One views it as a reminder of the ongoing importance of customary law when treaty law does not apply and ensures compliance with humanitarian principles and public conscience. The other faction considers the principles referred to in the clause to be derived from three independent sources: established customs, humanitarian principles, and the dictates of public conscience. We believe the latter to be entirely accurate, as the mentioned sources provide the ethical foundations for hostile operations.
- Implementation of International Humanitarian Law Rules: The practical application of international humanitarian law rules requires states parties to the four Geneva Conventions and the First and Second Additional Protocols, as well as specialized conventions, to undertake several commitments.
- Commitment to guarantee and respect international humanitarian law: States parties pledge to respect and implement the obligations they have undertaken. Fulfillment involves issuing instructions to their armed forces that comply with the rules set out in the texts of international humanitarian law[9]. The International Court of Justice affirmed that this principle constitutes a well-established rule of customary law and rises to the level of an obligation erga omnes, thus requiring all states to respect it and even compelling parties to any armed conflict to respect it as well.

Commitment to provide humanitarian assistance: Providing humanitarian assistance to victims of international and non-international armed conflicts has become a established practice in international law. Offering humanitarian aid does not necessarily mean resolving the issue of whether it is a right or a duty.

We believe that the best way to overcome any issues is to institutionalize the provision of assistance by entrusting it to neutral and objective organizations.

THE SECOND TOPIC INTERNATIONAL LEGAL REGULATION OF CYBER WARFARE

The international regulation of cyber warfare is a complex and evolving are of law. At present there is not a convention specially addressing cyber warfare in the same way that there are conventions regulating traditional forms of warfare, such as the Geneva and the Hague conventions. However, governmental efforts has led to a manuel providing a valuable guidance on how existing law applies to cyber warfare.

First requirement Scientific and technological advancement in warfare

The scientific and technological advancement in the methods and means of warfare have significantly transformed the landscape of modern armed conflicts. Cyber warfare encompasses a wide rang of activities, including hacking, malware deployment, and network exploitation, which can have significant implications for national security and defence.

First section: The emergence of cyber warfare

The operations on the internet can raise humanitarian concerns, especially when their effects are not limited to data on computers or computer systems but aim to create an impact in the real world. For example, hacking computer systems to control air traffic, oil pipelines, nuclear power stations, monitoring air, land, and sea traffic, and dams. Therefore, the potential impact of such operations would be highly dangerous, leading to catastrophic events such as aircraft collisions, release of toxic substances from chemical factories, or disruption of critical infrastructure like water and electricity supply networks, with civilians being the main victims of these operations.

Attacks against the internet are diverse and varied, but what concerns us in this context are attacks directed against internet networks. These attacks can be executed through several means such as viruses, computer worms, data collection operations, communication jamming devices, wireless data theft, suspicious counterfeit computer software, electromagnetic pulse weapons, computer reconnaissance tools, networks, and integrated parcel time bombs.

In 2007, Estonia suffered significant cyber attacks that lasted for several days. Similar attacks occurred during the conflict between Russia and Georgia in 2008, where Russia resorted to cyber warfare to disrupt Georgia's communication systems. Likewise, Israel targeted the Syrian nuclear reactor project in Deir ez-Zor in 2007, launching a cyber attack on Syrian air defenses

to disable and jam them before initiating the attack. In 2010, the United States and Israel used the Stuxnet virus against Iran's nuclear program to impact uranium enrichment operations and centrifuge devices. The attack resulted in the disabling of over 1000 centrifuges by increasing their speed to dangerous levels, while simultaneously sending false information to the control room to make it appear as if the systems were functioning normally. These events underscored the importance of the cyber domain as a battlefield, prompting nations to enhance their military capabilities in this area, both offensively and defensively. The cyber space has become a theater of conflict akin to the air, space, land, and sea domains, with modern technology utilizing electronic networks as a means to conduct military operations.

second section: Definition of cyber warfare

Electronic warfare can be defined as attacks carried out using computers, networks, or related systems, aimed at disabling or destroying internet systems, properties, or computer functions of the adversary. This term is also used to refer to means and methods of combat consisting of operations in the electronic space that rise to the level of armed conflict or occur within the context intended in international humanitarian law[10].

The term cyber warfare encompasses a variety of practices and procedures designed to disrupt and impair the electronic systems and capabilities of an adversary. It involves protecting against hostile electronic surveillance, resisting it, and ensuring stability for friendly electronic systems. The utilization of electromagnetic energy within the realm of cyber warfare is deemed essential for impeding enemy movements and thwarting their exploitation of the electromagnetic spectrum.

Cyber warfare is categorized into two main types: First, Radiation warfare: It employs electromagnetic radiation to degrade the quality of hostile information and data, which are neutralized through radiation – based research methods. Second, Data warfare: It focuses on exploiting data without causing direct harm. It ceases once data exchange between communicating parties halts.

second requirement: Tallin manuel regulates cyber warfare

Today, countries are facing the challenge of applying the legal system to international cyber armed conflicts. Multilateral international agreements constitute the primary source of rules in public international law and its branches, known as "hard law." They are based on the consent and consensus of states regarding matters of concern to the international community. However, when consensus is lacking and gathering states in a multilateral agreement

becomes difficult, the vitality of the issue may require resorting to what is known as "soft law"[11].

Several countries have adopted initiatives at both the national and international levels. The European Union has focused its efforts on cybercrime when it adopted in 2013 the "Cyber Security Strategy and Directive," which focused on the specific dimension of "cyber" security. The most successful initiative is reflected in the Tallinn Manual, which indicates that international humanitarian law applies to cyber warfare and delineates the role that the rules of international humanitarian law will play in this field. NATO published the Tallinn Manual in 2013, consisting of 282 pages and containing 95 articles on the applicable international laws in the event of cyber wars and organizing rules of engagement online.

This manual is divided into two sections: the first deals with cyber security law, and the second with cyber warfare law. The Tallinn law acknowledges that electronic operations may constitute armed conflicts depending on the circumstances, especially the destructive effects of those operations.

First section: Jus ad bellum Law:

The United Nations Charter considers the use of force in international relations as illegitimate under Article 4, paragraph 2 of the Charter, except in two cases: first, authorization from the Security Council under Chapter VII after the exhaustion of peaceful means under Chapter VI; second, legitimate self-defense.

Tallinn Manual considers cyber-attacks as an illegitimate use of force under Article 11, whether immediate or eventual[12], thus granting the targeted state the right to lawful self-defense[13]. It obliges the state to ensure that the response is proportionate to the attack[14], whether it's individual or collective self-defense[15]. Here, the Security Council must classify the cyber-attack as a threat to international peace and security under Article 39[16], and then decide to activate the collective defense mechanism by launching a cyber-attack[17].

The Tallinn Regulation considers electronic attacks as an unlawful use of force, whether actual or potential. It grants the targeted state the right to lawful defense and imposes an obligation to ensure proportionate response. Lawful defense can be individual or collective, with activation of collective defense contingent upon a decision by the Security Council based on identifying the electronic attack as a threat to peace and international security.

second section: Regulation of Hostile Operations

The regulation confirms that international armed conflict occurs when electronic attacks commence between two or more states[18]. Electronic attacks are subject to laws of armed conflict[19], and leaders and perpetrators who commit war crimes bear criminal responsibility[20]. Participants in electronic warfare do not enjoy mercenary status and are not immune as non-combatants[21]. Civilian participants in hostile operations lose their civilian status.

The Tallinn Regulation delineates the rights and obligations of states in cases of electronic armed conflicts and clarifies how traditional laws of armed conflict apply to electronic operations. It aims to provide a legal framework for regulating armed conflicts in the digital age and to achieve a balance between rights and responsibilities for the involved parties[22].

The parties involved in electronic hostile operations are required to respect the principle of distinction between civilians and combatants[23]. Civilians must not be electronically targeted as they are protected entities[24]. Information networks, computers, and electronic network infrastructure are considered civilian objects and therefore cannot be the target of electronic attacks[25]. Civilian objectives include any targets that are not used for military purposes and can be destroyed, partially or entirely, or controlled to reduce the enemy's military strength. Thus, military objectives include computer systems, electronic networks, and infrastructure for regular or optical cable networks[26]. Additionally, parties engaged in electronic hostile operations are prohibited from targeting civilians, civilian objects, places of worship, essential civilian items, dams, electricity, telephone networks, and nuclear power stations[27].

The Tallinn Manual emphasizes the possibility of applying the principle of distinction to electronic attacks. It states that civilians or groups must not be targets of electronic attacks. In cases of doubt about an individual's status as a civilian or military personnel, they are considered civilians. It specifies the following categories as legitimate targets during electronic armed conflicts: Armed forces, Members of organized armed groups, Civilians directly participating in hostilities and Participants in popular uprisings or international armed conflicts[28].

The Tallinn Manual stipulates that civilians are entitled to protection during periods when they are not participating in hostile operations[29]. It prohibits attacks intended to spread terror among civilians[30]. And states that civilian objects, including computers, computer networks, and computer infrastructure,

may not be targeted in electronic attacks[31]. The provisions in this manual represent a theoretical application of the principle of distinction. International laws on armed conflict allow for the use of non-state actors. Governments can contract with companies possessing hacking capabilities and use their networks as legitimate combatants in "cyber" conflicts. Non-state actors participating in hostile activities may be granted authorization, but these hacking networks are not easily identifiable, their weapons are not visibly apparent, and they do not bear insignia or markings.

A personal computer involved in an attack may be commandeered by a state without the knowledge of its innocent civilian owner. In the event of apprehension of those managing the hacked networks, can they be prosecuted as war criminals? What about the owners of the computers? Additionally, the interconnectivity between civilian and military networks makes it difficult, if not impossible, to distinguish between them. The issue of distinguishing between civilian populations and combatants, and between civilian objects and military targets, is highly complex. Unlike traditional attacks where the attacker is physically distant from the targeted location, in cyberattacks, it becomes impossible to distinguish between combatants and civilians. An example of this is the exposure of states to unknown-source attacks such as drone strikes[32]. Moreover, applying the legal definition of military targets in the electronic domain would render every electronic entity a legitimate military target. Every element of electronic infrastructure is dual-use. Additionally, the military extensively utilizes the same electronic infrastructure used for civilian purposes[33].

Given the interconnected nature of computer networks, it is inconceivable to target one part of the network without affecting the rest, whether it is an electronic attack or a conventional attack. In the explanations of the Tallinn Manual[34], the International Group of Experts believes that determining the nature of the network, whether military or civilian, is done by studying each case separately due to the absence of a standard defining the nature of the targeted network. In fact, this criterion is vague and subjective from the attacker's perspective, as it can paralyze the infrastructure of a state due to its own criteria, considering the targeted infrastructure a legitimate military target from its point of view. The Tallinn Manual considered civilian objects to be all objects that are not military targets, while military targets are those objects that, by their nature, location, purpose, or use, contribute effectively to military action. Their total or partial destruction, seizure, or disabling in the prevailing circumstances then constitutes a definite military advantage[35].

Military targets may include computers, computer networks, and computer infrastructure. It is certain that infrastructure with dual use is the primary tool in cyber warfare, and by destroying it partially or completely, it will lead to a definite military advantage. This mirrors the standards used against Iraq during the embargo, where Iraq was prevented from importing pencils under the pretext of dual use. Objects used for both civilian and military purposes, such as computers, computer networks, and electronic infrastructure, automatically become legitimate military targets. For example, a radar system used to monitor civilian ships and aircraft becomes a target if it is used to monitor any military aircraft or ship, even though its function is to monitor these vehicles regardless of their classification.

Conclusion

In conclusion, the following results can be drawn from this research paper:

- We believe that the fundamental principles of humanitarian law apply to cyber warfare, especially regarding the protection of civilians and civilian objects, which prohibits causing harm to computer systems, information networks, and optical fiber networks that serve public utilities.
- The First Additional Protocol of 1977, annexed to the 1949 Geneva Convention, stipulates in Article 36 under the category of new weapons, that when studying, developing, or acquiring new weapons or methods of warfare, consideration should be given to whether it is militarily feasible under this protocol or any other rule of international law to which the high contracting party is committed. This text indicates the applicability of international humanitarian law to cyber warfare.
- The advisory opinion of the International Court of Justice on the legality of the threat or use of nuclear weapons, states that Article 51 of the UN Charter prohibits the use of force regardless of whether it is with traditional or non-traditional weapons, including nuclear weapons, as humanitarian principles and rules were established before nuclear weapons. However, there is no reason to distinguish between nuclear weapons and electronic weapons in terms of the time they were introduced, which means the possibility of applying international humanitarian law to them.
- The Tallinn Manual serves as a flexible basis for regulating electronic armed conflicts, as it can help overcome the major disputes between major powers by proposing a solution that could potentially form the basis for a future multilateral international agreement.

- It is necessary to include cyber warfare within the concept of aggression, and the affected states have the right to legitimate defense as stipulated in Article 51 of the UN Charter.
- One of the most significant issues raised by cyber warfare is the difficulty in identifying the actor or perpetrator of cyber attacks, thus making it impossible to establish international responsibility in case of violations of the rules of international humanitarian law.

Bibliography List

- Kittichaisaree, Kriangsak, Public International Law of Cyberspace, Law, Governance and Technology Series 32, 1st edition, 2017.
- Roscini, Marco, World Wide Warfare –Jus ad bellum and Use of Cyber Force, Max Blank yearbook of United Nations Law, Volume 14, 2010.
- Jensen, Eric Talbot, Cyber Warfare and Precautions against the Effects of Attacks, Texas Law Review, Volume 88, 2010, 1533- 1569, P 1542 .
1. - Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.
2. - United Nations charter.
- The First Protocol of 1977 relating to the protection of victims of international armed conflicts.

Footnotes:

[1] - Criminalizing war and the resort to the use of force has been a lengthy interconnected process. First, the right of states to use force, i.e., resort to war, was restricted in the Covenant of the League of Nations in 1920. Later, the use of force was criminalized and prohibited under the Briand-Kellogg Pact in 1928. All countries of the world joined it, confirming a general international consensus on rejecting and prohibiting the use of force in international relations. The United Nations Charter reaffirmed this rule, as Article 4, paragraph 2, emphasizes that member states shall refrain from the use of force in their relations with other states.

[2] - See Article 51 of the United Nations Charter.

[3] - See Articles 43 -48 of the United Nations Charter.

[4] - Imperative rules are associated with the concept of the international public order and are defined as the accepted and recognized rule by the international community, meaning all states, as a rule that cannot be invalidated or modified into another rule of international law with the same character. Roberto Ago considers imperative rules to include fundamental rules related to the preservation of peace, such as rules prohibiting the use of force, as well as

fundamental rules of a humanitarian nature like the prohibition of genocide, slavery, racial discrimination, and the protection of basic human rights in peacetime as well as during war.

[5] - See Article 48 and 57 of Additional Protocol I.

[6] - See Article 35 of Additional Protocol I.

[7] - "Fyodor Martens" is one of the most prominent Russian jurists who served as the Imperial Russian Minister to the Hague negotiations in 1899.

[8] - The Martens Clause was included in the Preamble of the 1899 Hague Convention II concerning the Laws and Customs of War on Land, the 1907 Hague Convention VI concerning the Laws and Customs of War on Land, and was reintroduced in Additional Protocol I in Article 1 Paragraph 2.

[9] - See Article 1 of the 1907 Hague Convention and Article 1 of Additional Protocol I 1977.

[10] - Kittichaisaree, K., (2017), Public International Law of Cyberspace, Law, Governance and Technology, Series 32, P.154.

[11] - Soft law is defined as a set of rules operating in public international law that govern the behavior of states without constituting an independent source of law. In this sense, it closely resembles other sources, particularly those additional sources introduced by legal scholars, which are not explicitly mentioned in Article 38 of the Statute of the International Court of Justice, such as humanitarian considerations and legitimate interests. Humanitarian considerations refer to a set of human values protected by legal principles, although closely related to general legal principles or considerations of justice, they differ and stand apart in that they do not require justification of their legitimacy.

[12] - See Article 15 of the Tallinn Manual.

[1313] - See Article 13 of the Tallinn Manual.

[14] - See Article 14 of the Tallinn Manual.

[15] - See Article 16 of the Tallinn Manual.

[16] - See Article 18 of the Tallinn Manual.

[17] - See Article 19 of the Tallinn Manual.

[18] - See Article 22 of the Tallinn Manual.

[19] - See Article 20 of the Tallinn Manual.

[20]- See Article 26 of the Tallinn Manual.

[21] - See Article 28 of the Tallinn Manual.

[22] - See Article 29 of the Tallinn Manual.

[23] - See Article 31 of the Tallinn Manual.

[24] - See Article 35 of the Tallinn Manual.

[25] - See Article 37 of the Tallinn Manual.

[26] - See Article 38 of the Tallinn Manual.

[27] - See Article 47 of the Tallinn Manual.

[28] - See Article 96 of the Tallinn Manual.

[29]- See Article 96 of the Tallinn Manual.

[30] - See Article 98 of the Tallinn Manual.

[31] - See Article 99 of the Tallinn Manual.

[32] - Marco Roscini,World Wide Warfare –Jus ad bellum and Use of Cyber Force,Max Blank yearbook of United Nations Law,Volume 14, 2010, p. 88

[33] - Jensen,E., Cyber Warfare and Precautions against the Effects of Attacks, Texas LawReview, Volume 88, 2010, P 1533- 1569, P 1542.

[34] - See Article 99 of the Tallinn Manual.

[35] - See Article 100 of the Tallinn Manual.